UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Augusto Jun Devegili

Farnel: Uma Proposta de Protocolo Criptográfico para Votação Digital

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Prof. Dr. Ricardo Felipe Custódio

Florianópolis, Março de 2001

Farnel: Uma Proposta de Protocolo Criptográfico para Votação Digital

Augusto Jun Devegili

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação na área de Sistemas de Computação e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Dr. Ricardo Felipe Custódio

Prof. Dr. Fernando Ostuni Gauthier

Banca Examinadora

Prof. Dr. Luiz Carlos Zancanella

Prof. Dr. Aires José Rover

Prof. Dr. Antonio Alfredo Ferreira Loureiro

A vontade do povo é o fundamento da autoridade dos poderes públicos e deve exprimir-se através de eleições honestas a realizar periodicamente por sufrágio universal e igual, com voto secreto ou segundo processo equivalente que salvaguarde a liberdade de voto.
(Declaração Universal dos Direitos Humanos, Artigo 21, Parágrafo 3)

Ofereço esta dissertação a meus pais, Yoshiko e Arnildo Devegili, que propiciaram a base necessária para que eu chegasse a esta etapa da minha vida acadêmica.

Agradecimentos

Em primeiro lugar, agradeço o professor Ricardo Felipe Custódio, que extrapolou sua tarefa de orientador e foi, acima de tudo, um grande companheiro durante as atividades de mestrado.

Agradeço também os professores Aires José Rover (CCJ/UFSC), Antônio Alfredo Ferreira Loureiro (DCC/UFMG), Júlio Felipe Szeremeta (INE/UFSC), Luiz Adolfo Olsen da Veiga (CCJ/UFSC) e Luiz Carlos Zancanella (INE/UFSC) pelas críticas e sugestões ao trabalho, sempre pertinentes.

À equipe do LabSEC, colegas diários desta empreitada, meus agradecimentos pelas conversas, discussões, trabalho conjunto e companheirismo: Andrea Vergara, Jean Everson Martina, Juliana Eyng, Júlio da Silva Dias, Luciana Schmitz, Luciano Ignaczak. Aos Ostraconianos, meu agradecimento especial: Carlos Eduardo Mazzi, Fabiano Castro Pereira e John Cleber Jaraceski.

Houve um certo grupo de espanhóis que fez-me lembrar de que há vida além da universidade: Cristina Nieto, Mariano Campoy, Mònica Palacios, Santiago Cortegoso; em especial, Eugenia Rodríguez e Jaime Ferragut. *¡Hasta luego!*

Também preciso agradecer minhas amizades na Brasnet pelas longas conversas nas madrugadas onde pude relaxar a tensão e repor energias: Beatrice_, fake, Licurgo, Logician, Moondog, MyDyingBride, rolls, Sardaukar e nightZ.

Uma vez mais, agradeço meu orientador, professor Ricardo Felipe Custódio. Pelas discussões sobre mestrado e doutorado, matemática, método científico, didática no ensino superior, papel da universidade, pesquisa no Brasil, e a vida em geral: meu muito obrigado. Infinita é minha dívida, assim como meu apreço.

Sumário

Lista de Figuras

Resumo

Este trabalho caracteriza os sistemas de votação digital, em que a mobilidade dos eleitores é considerada um requisito importante, contrastando com o atual sistema de urna eletrônica utilizado nas eleições oficiais no Brasil. A votação digital permite sua realização através de redes de computadores como a Internet. É proposto e analisado o protocolo Farnel, um novo protocolo criptográfico a ser usado em votações digitais que contempla vários requisitos de segurança, e também é discutida a arquitetura necessária para a implementação de tais sistemas de forma a propiciar exeqüibilidade e praticidade em sua administração.

Palavras-chave: votação digital, protocolos criptográficos, criptografia aplicada.

Abstract

This dissertation describes digital voting schemes, where voters mobility is considered an important requirement, as opposed to the current electronic ballot system used in official elections in Brazil. Digital voting schemes can be implemented using computer networks such as the Internet. Farnel, a new digital voting cryptographic protocol, is proposed and analysed in regard to several security requirements, and the required architecture for implementing such schemes is discussed in order to provide feasibility and practicality in their management.

Keywords: digital and electronic voting, cryptographic protocols, applied cryptography.

Capítulo 1

Introdução

1.1 Motivação

É incontestável o aumento da utilização da Internet pela população em geral, o que tem provocado mudanças nas relações sociais e econômicas. Uma das principais vantagens da Internet, e também conseqüência da utilização de redes de computadores, é que redes propiciam a mobilidade da informação e, por conseguinte, das próprias pessoas. Utilizando seu computador pessoal em casa, um indivíduo pode fazer transações bancárias, comprar produtos, estudar e pesquisar informações em enciclopédias, visitar museus e comunicar-se com pessoas em lugares distantes. Empresas podem fazer tanto marketing quando venda a consumidores diretamente pela Internet *(business-to-consumer)*, ou então negociar diretamente com seus parceiros *(business-to-business)*. O governo aproxima-se dos cidadãos através do *e-government*. A recente integração entre Internet e dispositivos móveis de massa, tais como os telefones celulares, tende a acentuar consideravelmente este cenário.

Outra possível forma de interação social utilizando a Internet é a votação digital[1]. Votação é o ato de escolher uma opção dentre várias. Uma votação digital é conduzida por meio de redes de computadores – como a Internet –, beneficiando-se das vantagens

[1] Apesar de o termo mais difundido na comunidade científica internacional ser votação eletrônica (*electronic voting*), neste texto o termo votação digital é utilizado para caracterizar a diferença com relação ao processo de votação eletrônica atualmente utilizado no Brasil nas eleições para cargos públicos.

oferecidas por este meio de comunicação. A disponibilização de processos de votação em larga escala cria novas possibilidades de democracia: além das tradicionais eleições para cargos públicos, torna-se mais simples executar pesquisas de opinião e decisões em grupo. A democracia direta poderia ser praticada com o advento da ubiqüidade da Internet: no lugar de representantes públicos tomarem as decisões referentes à Nação, a própria população votaria tais decisões.

Considerando o valor das informações trafegadas na Internet, percebe-se facilmente a necessidade de garantir a segurança destas informações e, conseqüentemente, a segurança das entidades envolvidas: pessoas, empresas e instituições. O CERT (*Computer Emergency Response Team*) teve um aumento de aproximadamente 120% no número de notificações de incidentes de segurança entre o ano 1999 e ano 2000 [CER01].

Segurança é um requisito essencial em sistemas de votação digital, pois é necessário garantir a correta identificação de cada indivíduo, ao mesmo tempo em que seu anonimato é preservado e seu voto permanece secreto; é necessário que a apuração seja feita de forma correta e que sejam evitadas (ou detectadas) quaisquer corrupções no processo de votação. Um esquema de votação digital que contemple estes requisitos de segurança é complexo [RBR98], exigindo protocolos e ferramentas baseadas em criptografia para atingir os resultados esperados. Este trabalho objetiva estudar e avaliar um modelo de votação digital que leve em consideração variados requisitos de segurança.

1.2 Justificativa

A votação digital propicia a mobilidade dos votantes, os quais podem usar agentes qualificados (tais como navegadores WWW ou dispositivos móveis) para efetuar seu voto. Um modelo completo de votação digital permite que seja verificada a acuracidade da apuração dos votos, fato este necessário à aceitação deste modelo. Como a apuração é realizada de forma computacional, tende-se a agilizar o processo e diminuir a probabilidade de erros. Por outro lado, presume-se que o maior problema para a plena aceitação de modelos de votação digital seja cultural. O fato de o voto estar trafegando dentro de uma rede de computadores tende a deixar preocupados e com desconfiança os

indivíduos mais leigos, assim como os mais céticos. À parte da excelência científica e tecnológica, há que se cuidar da questão cultural.

Farnel, o protocolo proposto nesta dissertação, procura mimetizar o processo de votação existente no Brasil antes do advento da urna eletrônica. São estabelecidas correlações com a mesa da seção eleitoral (composta pelo presidente e pelos mesários), a lista de eleitores onde cada eleitor assina antes de obter a cédula em branco, a urna onde são colocadas as cédulas preenchidas e o recibo que cada eleitor recebe para comprovar sua presença no local de votação.

Espera-se que um modelo de votação digital similar ao modelo de votação tradicional gere um maior sentimento de confiança por parte da população em geral.

1.3 Organização do texto

O texto está estruturado da seguinte forma: no capítulo 2, o problema de votação digital é caracterizado considerando-se duas de suas possíveis formas: eleições oficiais e tomadas de decisão. O capítulo 3 descreve de forma breve os principais fundamentos de criptografia e o capítulo 4 ilustra protocolos baseados em criptografia que são úteis ao desenvolvimento de modelos de votação digital segura. O capítulo 5 apresenta o modelo de votação digital e enumera algumas propostas encontradas na revisão bibliográfica, enquanto que o capítulo 6 apresenta o protocolo Farnel. O capítulo 7 tece considerações finais acerca do trabalho desenvolvido.

Capítulo 2

Caracterização do Problema

A votação digital é um modelo computacional sistema computacional que reflete diferentes processos de votação encontrados no mundo físico. Sendo um modelo computacional, é mister compreender a estrutura e a dinâmica de diversos processos de votação, e a partir deste entendimento conceber um modelo que atenda aos requisitos funcionais e não-funcionais necessários à correta implementação.

2.1 Eleições Oficiais

As eleições oficiais são aquelas de caráter nacional ou regional em que a população elege os representantes para cargos oficiais e públicos. Dada a importância deste tipo de votação, deve-se considerar com extrema importância a segurança do processo, bem como flexibilidade e rapidez.

Com a utilização da urna eletrônica (e conseqüentemente voto eletrônico) nas eleições brasileiras, esperava-se um aumento da segurança no processo eleitoral. No seu discurso de posse, o Exmo. Sr. Ministro Carlos Velloso afirmou: "Estamos convencidos de que essas fraudes serão banidas do processo eleitoral brasileiro no momento em que eliminarmos as cédulas, as urnas e os mapas de urna, informatizando o voto." [CAM97]. No entanto várias críticas têm sido feitas à urna eletrônica [FIL99]: a validação dos programas contidos na urna eletrônica, a ausência de fiscalização ou recontagem na

apuração de uma urna, a impossibilidade de o eleitor conferir seu voto (ou seja, ter a certeza de que o seu voto foi corretamente inserido na urna) e o fato de o conteúdo do voto e a identificação do eleitor estarem disponíveis simultaneamente na mesma memória de computador, o que poderia levar à quebra do sigilo do voto.

Pode-se destacar as seguintes etapas no processo de uma eleição pública: o alistamento dos eleitores, a configuração da eleição, a execução da eleição e a apuração e publicação dos resultados.

2.1.1 A Legislação Eleitoral

A legislação eleitoral do Brasil baseia-se no Código Eleitoral instituído pela Lei 4737 de 15 de julho de 1965 [BRAa]. Além desta lei, existem outras leis, leis complementares e decretos-lei que em conjunto definem a atual legislação eleitoral.

A lei 9504 de 30 de setembro de 1997 [BRAb] regulamenta o voto eletrônico por meio dos seguintes artigos:

- **Art. 59:** possibilidade de utilização de sistema eletrônico
- **Art. 60:** voto de legenda no sistema eletrônico
- **Art. 61:** responsabilidade da urna eletrônica em relação à contabilização, sigilo e inviolabilidade, bem como possibilidade de fiscalização
- **Art. 62:** eleitores autorizados a votar em uma seção com urna eletrônica
- **Art. 66:** fiscalização do processo de votação e apuração das eleições, sendo garantido o conhecimento dos programas de computador utilizados.

Houve várias resoluções baixadas pelo TSE para regulamentar alguns aspectos específicos da utilização da urna eletrônica na eleição. As seguintes resoluções referem-se às eleições municipais de 2000:

- **Resolução 20.563 de 27/03/2000:** regulamenta os atos preparatórios, a recepção de votos e as garantias eleitorais [ELEa];

- **Resolução 20.565 de 27/03/2000:** regulamenta a apuração e a totalização dos votos e a proclamação e a diplomação dos eleitos [ELEb];

- **Resolução 20.633 de 23/05/2000:** estabelece os modelos e uso dos lacres para urnas eletrônicas [ELEc];

- **Resolução 20.676 de 11/07/2000:** regulamenta a divulgação dos resultados [ELEd].

O projeto de lei do Senado SF PLS 194/99, submetido pelo senador Roberto Requião e atualmente em tramitação, objetiva promover alterações na Lei 9504/97 para "ampliar a segurança e a fiscalização do voto eletrônico" [BRAc]. As principais medidas apontadas por este projeto de lei são (i) a impressão do voto do eleitor e conseqüente verificação do resultado da urna eletrônica através da contagem dos votos impressos; e (ii) a desvinculação da identificação do eleitor com a urna eletrônica, evitando-se que seja possível relacionar o eleitor ao seu voto, bem como a ordem de identificação dos eleitores, a qual poderia ser utilizada para relacionar aos votos pela ordem de emissão dos votos.

2.1.2 Alistamento dos Eleitores

A Constituição Brasileira prevê a obrigatoriedade ou a opcionalidade de voto para os brasileiros, considerando fatores como faixa etária e deficiência física. Independentemente destas considerações, para que um indivíduo consiga votar ele deverá obter um título de eleitor junto ao Tribunal Regional Eleitoral. Este título é uma declaração de que o indivíduo está autorizado a votar, e o processo de obtenção do título é denominado alistamento.

Para a emissão do titulo de eleitor, é necessário que a pessoa se identifique com algum documento reconhecido pelo governo brasileiro como prova de identidade, tais como a carteira de identidade, o certificado de quitação militar ou certidão emitida no registro civil. A competência da organização e manutenção do cadastro de eleitores de cada unidade de federação é do Tribunal Regional Eleitoral. As zonas eleitorais são

responsáveis pelo cadastramento dos eleitores a ela associados [CAM97]; um eleitor sempre está relacionado a uma zona eleitoral específica.

2.1.3 Configuração da eleição

Chamada de "atos preparatórios" pela regulamentação do Tribunal Superior Eleitoral, a etapa de configuração é a responsável pela preparação do ambiente necessário à execução da eleição.

Os juízes eleitorais são os responsáveis por elaborar a lista de candidatos, as quais são processadas por um sistema especializado para gerar os cartões de memória de carga e de votação, bem como os disquetes das urnas eletrônicas. A carga destes dados na urna eletrônica é feita pelos próprios juízes eleitorais, sendo permitida a presença de fiscais e delegados dos partidos políticos ou coligações. Logo em seguida as urnas são lacradas e permanecem sob vigilância até o momento de serem distribuídas aos locais de votação [ELEa].

2.1.4 Execução da eleição

O período de votação é pré-determinado e inalterável[1].

O subprocesso de execução da eleição, ou seja, da votação em si, ocorre da seguinte forma:

- o eleitor apresenta à mesa receptora um documento de identidade (o qual não precisa ser o título de eleitor), o qual é verificado na folha de votação e no cadastro dos eleitores constante na urna eletrônica;
- o eleitor assina a folha de votação;
- o presidente da mesa autoriza o eleitor a votar (através de dispositivo especial instalado na mesa receptora);

[1] A votação pode estender-se caso haja eleitores que tenham chegado ao local de votação até o término do período de votação porém a urna eletrônica ainda estava em uso.

- o eleitor efetua seu voto.

Ao fim do período de votação, o presidente da mesa dirige-se à urna eletrônica e digita uma senha específica para encerrar a votação. É emitido o boletim da urna em cinco vias, e é retirado o disquete da urna eletrônica contendo os dados da eleição. Os boletins de urna são assinados pelo presidente, primeiro secretário e eventualmente por fiscais de partidos políticos; são identificados os eleitores faltosos e registradas as ocorrências que porventura aconteceram durante a votação.

De acordo com [ELEa]:

> "Art. 43. O sigilo do voto é assegurado mediante as seguintes providências:
>
> I. uso de urna eletrônica e, se for o caso, de cédulas oficiais;
>
> II. uso de sistemas de informática exclusivos da Justiça Eleitoral;
>
> III. isolamento do eleitor em cabina indevassável para o só efeito de indicar, na urna eletrônica de votos ou na cédula, o candidato de sua escolha;
>
> IV. verificação da autenticidade da cédula oficial à vista das rubricas, se for o caso;
>
> V. emprego de urna que assegure a inviolabilidade do sufrágio e seja suficientemente ampla para que não se acumulem as cédulas na ordem em que forem introduzidas (Código Eleitoral, art. 103, I a IV)."

2.1.5 Apuração e publicação dos resultados

O boletim emitido pela urna eletrônica ao final da votação contém as seguintes informações: data da eleição, identificação do município, da zona eleitoral e da seção eleitoral, horário de encerramento da votação, código de identificação da urna eletrônica, número de eleitores aptos, número de votantes, votação individual de cada candidato, votos de cada legenda partidária, votos nulos, votos em branco e soma geral dos votos [ELEb]. Todas as vias do boletim são assinadas pelo presidente da mesa, pelo primeiro secretário e pelos fiscais que assim o desejarem.

2.2 Tomada de Decisão

Define-se tomada de decisão como a manifestação de opiniões sobre um determinado assunto por uma comunidade específica de indivíduos, e o conseqüente estabelecimento de uma decisão com base nestas opiniões. Em muitos casos a opinião é expressa como um "sim" ou "não" referente a uma pergunta, mas não se restringe a esta situação.

Há um amplo conjunto de casos em que é possível aplicar a tomada de decisão. Como exemplos, pode-se citar:

- Um grupo de acionistas que, a par de um projeto na empresa, precisa decidir se será liberado o financiamento para este projeto;
- O mesmo grupo de acionistas precisa eleger (decidir) o novo diretor-presidente da empresa;
- A diretoria de uma empresa, ao ter conhecimento do resultado da visita de um consultor que demanda com urgência a liberação de informações confidenciais, precisa decidir se tais informações serão liberadas;
- A coordenação de um curso quer que os alunos manifestem sua opinião sobre o andamento de uma disciplina para decidir eventuais alterações na disciplina. Somente os alunos atuais devem opinar, e este ato deve ser feito de forma anônima;
- A associação dos professores de uma universidade precisa obter os votos dos professores para decidir se haverá greve. Nem todos os professores desejam deslocar-se até o local da reunião, porém querem manifestar sua opinião e votar pela decisão de greve.

Considerando-se o último exemplo de tomada de decisão, pode-se delinear o processo da seguinte forma:

- A associação de professores define quais os indivíduos que têm direito a voto. Neste caso, a associação possui a lista dos professores da universidade;

- A associação também define qual o tema da decisão (greve?) e as opções possíveis (sim ou não);
- Tem início o processo de votação;
- Os professores votam;
- Encerra-se a votação;
- Apura-se o resultado;
- O resultado é divulgado.

Uma tomada de decisão pode ser encerrada em um determinado prazo, ou quando um número limite de indivíduos efetuou seu voto. É feita então a contagem dos votos para identificar qual a decisão que deverá ser escolhida.

Nem todas as tomadas de decisão exigem anonimato. Em alguns casos, pode-se até exigir que o voto seja conhecido pela comunidade envolvida.

Capítulo 3

Fundamentos de Criptografia

Criptografia pode ser definida como a arte e ciência de garantir a segurança de mensagens [SCH96] constantes na comunicação entre uma entidade emissora e uma entidade receptora. A mensagem original gerada pela entidade emissora é denominada texto plano. O texto plano, ao ser processado por um algoritmo de criptografia, gera o texto cifrado, ininteligível para quem não está autorizado a conhecer o conteúdo do texto plano. A obtenção do texto plano original a partir do texto cifrado é denominada descriptografia. A Fig. 3.1 ilustra este processo.

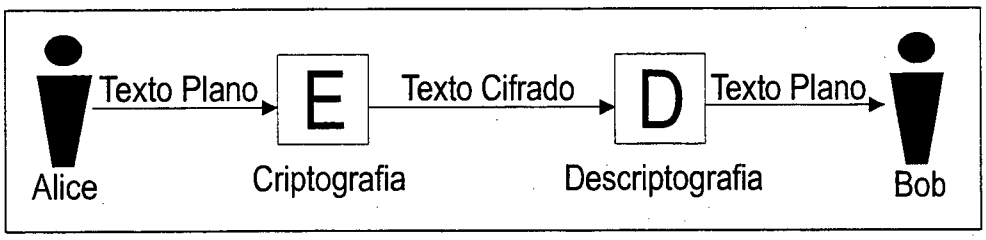

Figura 3.1: Processo de criptografia e descriptografia

Nos textos sobre criptografia, usualmente a entidade emissora é denominada Alice, e a entidade receptora é denominada Bob.

Por intermédio de criptografia, obtém-se:

- **Confidencialidade** Não é possível que uma terceira entidade consiga obter o texto plano correspondente ao texto cifrado que está sendo transmitido entre Alice e Bob;

- **Identificação** Deve ser possível que Bob consiga verificar a identidade de Alice, isto é, ter garantia de que é realmente Alice quem está enviando a mensagem. O mesmo deve ser válido para Alice com relação a Bob;

- **Integridade** Deve ser possível para Bob ter garantia de que a mensagem que ele está recebendo é a mesma mensagem que Alice enviou, i.e., se uma terceira entidade adulterou a mensagem, deve ser possível que Bob consiga detectar esta adulteração;

- **Não-repúdio** A partir do momento em que Alice envia uma mensagem a Bob, não deve ser possível que Alice negue a Bob que tenha enviado tal mensagem.

Para a utilização do processo de criptografia e descriptografia são necessários algoritmos criptográficos (comumente denominados cifradores) e chaves de criptografia.

O cifrador é um algoritmo que, com base em substituições e permutações ou funções e operadores matemáticos, transforma o texto plano em texto cifrado.

Se a segurança de um algoritmo de criptografia baseia-se no segredo do algoritmo, ele é dito *restrito*; todavia, estes cifradores não são largamente utilizados [SCH96]. Nos cifradores modernos, segue-se o princípio de Kerckhoff, em que a segurança de um algoritmo de criptografia baseia-se no segredo das chaves envolvidas, e não no segredo do algoritmo em si [STI95].

A chave é um parâmetro do cifrador, independente do texto plano, que faz com que a saída do cifrador seja dependente do texto plano e da chave. O conjunto de possíveis chaves de um cifrador é denominado espaço de chaves.

De acordo com [STI95], um criptossistema é uma cinco-tupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ tal que:

- $\mathcal{P}$ é um conjunto finito de possíveis textos planos

- $\mathcal{C}$ é um conjunto finito de possíveis textos cifrados

- $\mathcal{K}$ é o espaço de chaves

- para cada $K \in \mathcal{K}$, há uma regra de criptografia $e_K \in \mathcal{E}$ e uma regra de descriptografia correspondente $d_K \in \mathcal{D}$. Cada $e_K : \mathcal{P} \rightarrow \mathcal{C}$ e $d_K : \mathcal{C} \rightarrow \mathcal{P}$ são

funcões tais que $d_K(e_K(x)) = x$ para cada texto plano $x \in \mathcal{P}$.

A diferença em como um criptossistema trata a relação entre os conjuntos $\mathcal{E}$ e $\mathcal{D}$ pode dividi-los em duas categorias de algoritmos de criptografia: os simétricos e os assimétricos.

3.1 Criptografia Simétrica

Em um criptossistema simétrico, a mesma chave que foi utilizada para criptografar o texto plano é utilizada para descriptografar o texto cifrado correspondente. Como a mesma chave é utilizada na criptografia e na descriptografia, diz-se que o criptossistema é simétrico. A chave desta categoria de criptossistemas é comumente denominada *chave secreta* (K_A).

Como a chave é a mesma, e_{K_A} é a aplicação da chave secreta ao algoritmo de criptografia, e d_{K_A} é a aplicação da mesma chave secreta ao algoritmo de descriptografia, conforme ilustra a Fig. 3.2. Na maioria dos cifradores simétricos, o algoritmo de criptografia e descriptografia é o mesmo, mudando-se apenas a maneira como é utilizada a chave secreta.

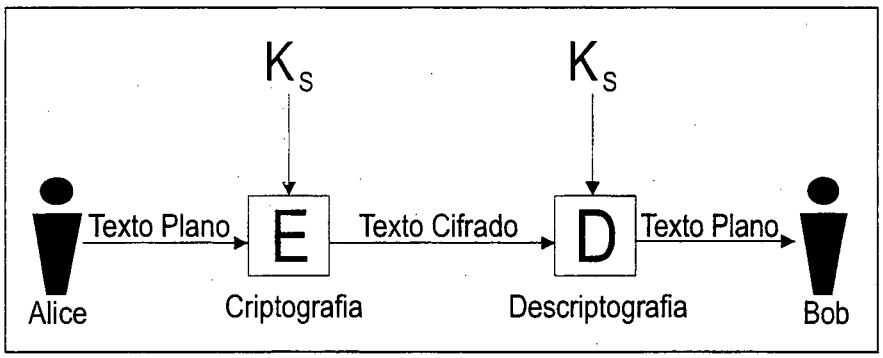

Figura 3.2: Utilização de chaves na criptografia simétrica

Para que a entidade emissora e a entidade receptora consigam estabelecer uma comunicação segura utilizando um sistema de criptografia simétrica, é necessário que as duas entidades tenham entrado previamente em acordo para definir qual a chave que deve

ser utilizada. Idealmente, a chave precisaria ser transmitida por um canal seguro, o que pode ser difícil de se conseguir.

Como exemplos de cifradores simétricos, pode-se citar os algoritmos DES, Blowfish, IDEA, CAST e RC5 [STA99].

3.2 Criptografia Assimétrica

Em um criptossistema assimétrico, utiliza-se um par[1] de chaves – uma delas é utilizada na criptografia, e a outra é utilizada na descriptografia. Uma das chaves é mantida em segredo, e é denominada *chave privada* (KR_A). A outra é amplamente divulgada, sendo denominada *chave pública* (KU_A) (Fig. 3.3).

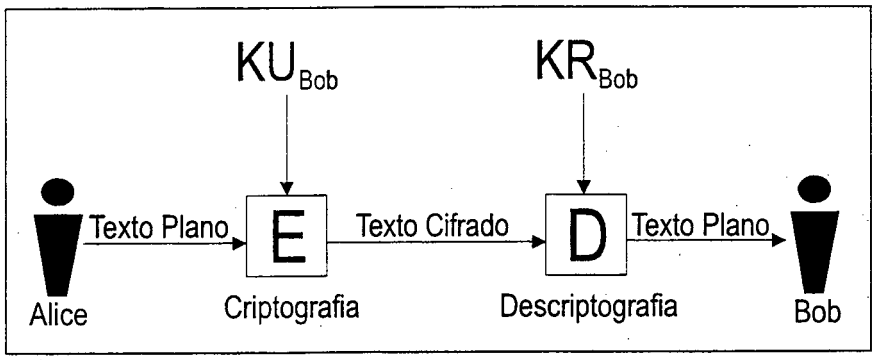

Figura 3.3: Utilização de chaves na criptografia assimétrica para obter confidencialidade

Neste caso, e_{KU_A} é a aplicação da chave pública de A ao algoritmo de criptografia, e d_{KR_A} é a aplicação da chave privada de A ao algoritmo de descriptografia. Há uma forte relação entre as duas chaves que compõem o par para permitir que $d_{KR_A}(e_{KU_A}(x)) = x$. Em alguns algoritmos, tanto a chave privada quanto a pública podem ser utilizadas para criptografia.

Como exemplos de cifradores assimétricos, pode-se citar os algoritmos RSA, ElGamal e Criptossistemas de Curvas Elípticas [STI95].

[1] Em alguns criptossistemas assimétricos é possível utilizar mais de duas chaves (e.g. seção 4.5).

3.2.1 RSA

RSA é um algoritmo de criptografia assimétrica cuja segurança baseia-se na dificuldade de se fatorar o produto de dois números primos grandes [DIF88]. As operações são executadas no anel $\mathbb{Z}_n$, onde n é obtido pela multiplicação de dois números primos.

O algoritmo funciona da seguinte forma [STA99]:

- Bob cria seu par de chaves a partir da escolha aletória de dois números primos grandes, p, q
- Bob calcula n tal que $n = p \times q$
- Bob calcula[2] $\phi(n) = (p-1)(q-1)$
- Bob escolhe um expoente e tal que $\gcd(\phi(n), e) = 1$ e $1 < e < \phi(n)$
- Bob calcula d tal que $d = e^{-1} \bmod n$
- A chave pública de Bob, KU_{Bob}, é a tupla $\{e, n\}$
- A chave privada de Bob, KR_{Bob}, é a tupla $\{d, p, q\}$

Alice envia uma mensagem criptografada para Bob calculando $c = m^e \bmod n$. Bob, para descriptografar a mensagem, calcula $m = c^d \bmod n$.

Formalmente, pode-se definir o algoritmo da seguinte forma [STI95]:

- Seja $n = pq$, onde p, q são primos.
- Seja $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$
- Define-se $\mathcal{K} = \{(n, p, q, d, e) : de \equiv 1 (\mathrm{mod} \phi(n))\}$
- Para $K = (n, p, q, d, e)$, defina-se $e_K(p) = p^e \bmod n$ e $d_K(c) = c^d \bmod n$

[2] A função $\phi(n)$ é denominada função totiente de Euler, e representa o número de inteiros positivos menores do que n e relativamente primos a n. A função $\gcd(a, b)$ representa o maior divisor comum dos números a e b. Dois números x, y são relativamente primos se o número 1 é o único número divisor de ambos, ou seja, $\gcd(x, y) = 1$.

- $c, p \in \mathbb{Z}_n$. Os valores e, n são públicos; os valores p, q, d são privados.

O algoritmo RSA pode ser atacado de três possíveis maneiras: força bruta, ataques matemáticos ou ataques de temporização [STA99]. Para proteger-se dos ataques de força bruta deve-se aumentar o tamanho da chave, ou seja, permitir um valor de n (d, e) maior. Em [LV00] propõe-se um modelo para sugerir o tamanho de chave apropriado para cada ano. Por exemplo, para o ano 2000 sugere-se um tamanho de chave de 952 bits para o RSA; para o ano 2010, 1369 bits.

Os ataques de temporização baseiam-se no tempo levado para efetuar os cálculos do algoritmo, do qual poder-se-ia derivar o tamanho dos fatores utilizados.

O principal ataque matemático ao RSA é baseado na tentativa de se fatorar n em seus dois fatores primos d, e. Obtendo-se d, e, facilmente obtém-se $\phi(n) = (p-1)(q-1)$ e conseqüentemente $d = e^{-1}(\mathrm{mod}\phi(n))$. Todavia, para um valor de n com fatores primos grandes, fatorização é um problema difícil [STA99].

3.3 Assinatura Digital

A assinatura digital é um algoritmo criptográfico com as seguintes características [SCH96]:

- **Identificação:** a assinatura garante a identificação do remetente e que ele deliberadamente assinou a mensagem;
- **Não-Falsificação:** a assinatura garante que o remetente, e ninguém mais, assinou a mensagem;
- **Unicidade:** a assinatura é parte de uma mensagem, e não pode ser reutilizada em uma mensagem diferente;
- **Integridade:** depois de uma mensagem ter sido assinada, ela não pode ser alterada;
- **Não-Repúdio:** a assinatura não permite que o remetente alegue não ter assinado a mensagem.

Uma assinatura digital pode ser obtida por meio da criptografia de um resumo[3] da mensagem com a chave privada da entidade que está assinando a mensagem: $S_A(M) = E_{KR_A}(H(M))$ [STA99].

Métodos de assinatura direta, em que estão apenas envolvidos o emissor e o receptor na comunicação, possuem uma fraqueza: como a validade da assinatura depende da chave privada do emissor (aquele que assina), ele pode enviar um documento e mais tarde afirmar que sua chave privada foi de alguma forma comprometida. Para resolver este impasse, existem protocolos para assinatura digital arbitrada, em que uma terceira parte, o árbitro, é reponsável por garantir a validade da assinatura [STA99].

Como exemplos de algoritmos de assinatura digital, pode-se citar o DSA [STA99] e o RSA [Cap. 3.2.1].

3.4 Certificados Digitais

Uma questão referente à utilização de criptografia assimétrica é a confiança na autenticidade da chave pública de uma entidade, i.e., como ter certeza de que uma chave pública realmente pertence à entidade?. Um certificado digital é uma associação entre a chave pública de uma entidade e atributos relacionados à sua identidade [FFW99]. A autoridade certificadora assina com sua chave privada o certificado digital, o qual contém, além da chave pública, informações a ela referentes, como por exemplo o nome da entidade à qual a chave pública está relacionada.

O certificado digital pode ser publicamente distribuído (por exemplo em um diretório X.500 ou LDAP). Quando uma entidade precisa verificar a chave pública de outra entidade, basta obter o certificado digital correspondente e validar a assinatura da autoridade certificadora. Confiando-se na autoridade certificadora, confia-se também nos certificados por ela emitidos.

O padrão mais reconhecido para certificados digitais é o X.509v3 (ISO/IEC/ITU-T) [FB97, ITU97a]. São padronizados o formato do certificado,

[3] O resumo também é denominado função de condensação ou função de caminho único, aqui sendo simbolizado pela função $H()$.

atributos, extensões e listas de revogação de certificados, as quais informam certificados que por algum motivo perderam a validade.

Para que tecnologias baseadas em certificados de chave pública sejam utilizadas em larga escala, é necessário um conjunto de serviços baseados no uso de autoridades certificadoras. Uma *infra-estrutura de chave pública* é um conjunto de padrões, autoridades certificadoras, estruturas de inter-relacionamento entre autoridades certificadoras, métodos para descobrir e validar caminhos de certificação, protocolos para operacionalização e protocolos para gerenciamento [FFW99].

Capítulo 4

Protocolos Criptográficos

Protocolo é um conjunto de passos durante a comunicação entre duas ou mais entidades, de forma a atingir um determinado objetivo [SCH96]. Um protocolo criptográfico é um protocolo que utiliza criptografia, e tem como requisito a condição de que nenhuma entidade deve conseguir fazer mais ou saber mais do que está especificado no protocolo. Protocolos criptográficos, com base em mecanismos como criptografia simétrica e assimétrica, funções de condensação e assinaturas digitais, fornecem os meios necessários para do desenvolvimento de aplicações seguras.

4.1 Comprometimento de Bit

O protocolo de comprometimento de bit é utilizado quando uma entidade deseja comprometer-se a uma informação perante outra entidade [SCH96], que só poderá verificá-la em um momento posterior. No exemplo abaixo, Alice compromete-se a uma informação perante Bob.

- Bob gera uma string com bits randômicos, denominada R, e a envia para Alice
- Alice cria uma mensagen que consiste do bit (b) que ela deseja comprometer concatenado com a string R enviada por Bob. O resultado da concatenação é criptografado com uma chave randômica K, e o resultado é enviado para Bob ($e_K(R, b)$)

Quando Alice desejar revelar a informação a Bob, o protocolo continua como segue:

- Alice envia a chave K para Bob
- Bob descriptografa a mensagem e o bit é revelado. Bob compara a string randômica para verificar a validade da mensagem.

Uma outra forma de implementar o protocolo de comprometimento de bit é através de funções de caminho único. A vantagem desta implementação é que Bob não precisa enviar quaisquer mensagens a Alice.

- Alice gera duas strings com bits randômicos, R_1 e R_2
- Alice cria uma mensagem com suas strings randômicas e o bit que ela deseja comprometer (R_1, R_2, b)
- Alice utiliza a função de caminho único na mensagem e envia o resultado a Bob, juntamente com uma das strings randômicas $(H(R_1, R_2, b), R_1)$

Para que Alice revele a informação, o protocolo segue:

- Alice envia a Bob a mensagem original (R_1, R_2, b)
- Bob utiliza a função de caminho único na mensagem e compara, juntamente com R1, com o valor e a string que ele recebeu na primeira etapa do protocolo.

4.2 Assinaturas Cegas

Assinaturas cegas foram propostas por David Chaum [CHA81] como uma técnica para que uma entidade consiga que outra entidade assine uma mensagem sem saber seu real conteúdo.

Considere-se o exemplo abaixo, utilizando RSA, em que Alice quer que Bob assine digitalmente uma mensagem sem conhecer o conteúdo dela.

A chave pública de Bob, KU_B, é composta pela tupla $\{e, n\}$. Sua chave privada, KR_B, é composta pela tupla $\{d, n\}$.

- Alice deseja que Bob assine cegamente a mensagem m
- Alice escolhe k (denominado fator de ocultação) tal que k é randômico, $1 < k < n$ e $\gcd(k, n) = 1$
- Alice calcula m' tal que $m' = m \times k^e \bmod n$
- Alice envia m' para Bob
- Bob assina $(m')^d \bmod n \Leftrightarrow (m \times k^e)^d \bmod n$
- Alice calcula $s = \frac{(m')^d}{k} \bmod n$; $s = m^d \bmod n$

$$
\begin{aligned}
(m')^d &= (m \times k^e)^d \bmod n \\
&= m^d \times k^{e^d} \bmod n \\
&= m^d \times k \bmod n
\end{aligned}
$$

$$
\begin{aligned}
\frac{(m')^d}{k} \bmod n &= \frac{m^d \times k}{k} \bmod n \\
&= m^d \bmod n
\end{aligned}
$$

4.3 Cortar-E-Escolher

A utilização isolada de assinaturas cegas não é prática porque Alice poderia, maliciosamente, fazer com que Bob assinasse uma mensagem qualquer, sem que Bob tenha garantias de que ele realmente concorda em assinar aquela mensagem. Para evitar esta situação, utiliza-se a técnica cortar-e-escolher [SCH96]:

- Alice cria n mensagens e as cega com diferentes fatores de ocultação
- Alice envia as n mensagens para Bob
- Bob escolhe randomicamente $n - 1$ mensagens e pede a Alice que revele os fatores de ocultação de cada uma delas
- Alice envia a Bob os fatores de ocultação apropriados

- Bob abre as $n-1$ mensagens e verifica que os conteúdos não são maliciosos
- Bob assina a mensagem restante e a envia para Alice.

Pode-se notar que variando-se n obtêm-se diferentes graus de certeza. A probabilidade de Alice conseguir enganar Bob é n^{-1}, ou seja, à medida que n aumenta, diminui a probabilidade de Alice agir maliciosamente. Em contrapartida, quanto maior for o valor de n, maior o tempo computacional necessário para efetuar o protocolo.

4.4 Redes de Misturadores

A comunicação anônima não é tarefa trivial em redes de computadores porque protocolos de rede incluem cabeçalhos nos datagramas contendo os endereços de origem e de destino. Redes de misturadores [CHA81] são consideradas a solução mais prática para este problema [RB99], sendo utilizadas para garantir a privacidade em comunicação pura, com aplicações em navegação na Web, eleições digitais e esquemas de pagamento [JAK98].

Um misturador é uma entidade que, além de receber e enviar mensagens, esconde a relação entre mensagens de entrada e mensagens de saída. As mensagens chegam aos misturador, são permutadas e o endereço de origem constante nos datagramas é substituído pelo endereço do próprio misturador. As mensagens de entrada, além da permutação, também sofrem algum processo de transformação antes de saírem do misturador. É necessário que todas as mensagens de saída tenham o mesmo tamanho para evitar que se consiga relacionar uma mensagem de saída à mensagem de entrada correspondente.

Para evitar que o misturador seja um ponto único de falha, é comum utilizar vários misturadores organizados em seqüência, formando uma rede de misturadores. Uma característica desta rede é que é necessário que apenas um dos misturadores seja honesto para evitar que se consiga relacionar as mensagens de entrada às mensagens de saída, mesmo que todos os demais misturadores sejam maliciosos.

Para detectar possíveis ataques a misturadores em uma rede de misturadores, um misturador pode criptografar as mensagens de entrada duas vezes, e permutar as listas

de mensagens de saída. O outro misturador pede então que ou o primeiro ou o segundo bloco de permutações e criptografias seja revelado, obtendo-se 50% de confiança de que o misturador é honesto. Este procedimento é repetido várias vezes para cada misturador.

4.5 Criptografia de Chave Pública com Múltiplas Chaves

É possível fazer uma generalização do algoritmo RSA para lidar com múltiplas chaves [SCH96] da seguinte forma: sejam p e q dois números primos. Deve-se escolher t chaves tais que $K_1 \times K_2 \times \cdots \times K_t \equiv 1 \bmod (p-1)(q-1)$, posto que $M^{K_1 \times K_2 \times \cdots \times K_t} \bmod n = M \bmod n = M$.

Considere-se o caso de Alice e Bob assinando um mesmo documento. São necessárias três chaves: $KR_A(K_1), KR_B(K_2), KU_{AB}(K_3)$. O procedimento para a múltipla assinatura e posterior verificação é o seguinte:

1. Alice assina o documento M e o envia para Bob
   $M' = M^{K_1} \bmod n$

2. Bob recupera o documento M a partir de M'
   $M = M'^{K_2 \times K_3} \bmod n$

3. Bob adiciona a sua assinatura
   $M'' = M'^{K_2} \bmod n$

4. Vera (qualquer entidade) verifica a assinatura
   $M = M''^{K_3} \bmod n$

Capítulo 5

Introdução à Votação Digital

Há várias possíveis abordagens no projeto de uma aplicação segura. É importante analisar o nível em que a segurança é implementada nestas aplicações, considerando-se o modelo de referência OSI ou, mais especificamente, o modelo Internet. A primeira abordagem diz respeito aos serviços de segurança oferecidos pelas camadas mais baixas, até a camada de rede (e.g. IPSEC [SMI97]). Tais serviços geralmente são inadequados porque dizem respeito somente ao tráfego de datagramas entre computadores, sem a diferenciação de quais datagramas estão relacionados a quais processos da camada de aplicação, e qual o protocolo necessário para a comunicação segura entre os dois processos. Uma outra possível abordagem é utilizar os serviços de segurança providos pela camada de transporte (e.g. SSL [SMI97]), responsável por oferecer comunicação confiável entre processos. Desta forma, obtêm-se serviços de autenticação, confidencialidade e integridade nesta comunicação. Por outro lado, a camada de transporte não compreende a semântica das TPDUs que são transferidas. Aplicações distintas possuem diferentes requisitos de segurança, os quais vão além dos serviços genéricos oferecidos pela camada de transporte. Conseqüentemente, torna-se necessária a definição de protocolos e mecanismos específicos a cada aplicação, e cuja responsabilidade é da camada de aplicação (Fig. 5.1).

Um sistema de votação digital pode ser definido da seguinte forma [RIE99]:

Um esquema de votação eletrônica é uma aplicação distribuída composta por

um conjunto de mecanismos e protocolos criptográficos que conjuntamente permitem que uma eleição seja realizada em uma rede de computadores, de forma segura, mesmo assumindo que participantes legítimos tenham comportamento malicioso.

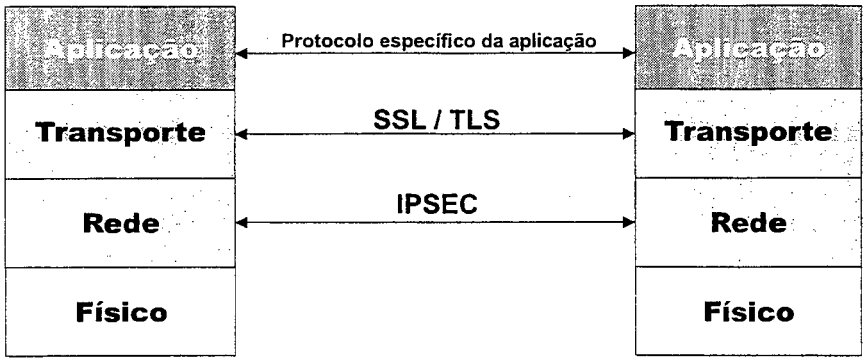

Figura 5.1: Camadas do modelo Internet e protocolos criptográficos relacionados

5.1 Processo de votação digital

Um sistema de votação digital não se limita apenas ao ato de o votante emitir seu voto, mas a todos os procedimentos envolvidos no processo:

- **Fase de configuração:** esta fase compreende a definição das características gerais de uma votação, tais como um identificador único para a votação e o período de alistamento e de votação. Além disso, são também definidas as categorias e opções que constarão na cédula de voto. A responsabilidade desta definição é de uma autoridade de votação denominada autoridade de configuração, a qual deve disponibilizar as informações em algum lugar público, tais como a World Wide Web ou diretórios ITU-T X.500 e LDAP.

- **Fase de alistamento:** nesta fase preliminar uma autoridade de votação, denominada autoridade de alistamento, é responsável por registrar todos os votantes autorizados a participar de uma votação. A relação de votantes, assim como as

informações de configuração, deve ser tornada pública para que, durante um certo período de tempo, os votantes possam verificar sua correta inclusão nesta relação e notificar a autoridade de alistamento caso haja divergências.

- **Fase de votação:** durante esta fase, cujo período foi previamente estabelecido pela autoridade de configuração, os votantes podem emitir seus votos a partir de agentes de usuário de votação. A cédula de votação contendo os votos é enviada a um centro de votação de forma anônima. O centro de votação mantém as cédulas em uma urna digital.

- **Fase de apuração:** após a fase de votação, o centro de votação pára de aceitar as cédulas, e inicia-se a fase de apuração dos votos. O resultado da apuração é disponibilizado de forma pública. São necessários mecanismos para detectar (e idealmente corrigir) qualquer corrupção durante a fase de apuração.

Diferentes esquemas de votação digital tratam de forma diversa as autoridades envolvidas nas várias fases [SCH96]. É possível que um esquema possua uma única autoridade que executa a funcionalidade de todas as autoridades – neste caso, esta autoridade é denominada autoridade de votação.

As fases de configuração e alistamento podem ser feitas de forma paralela. Todavia, é possível que a fase de alistamento necessite de informações definidas durante a fase de configuração, como por exemplo o identificador único da eleição [RIE99]. Como a fase de votação depende de todos os votantes terem-se alistado, ela é iniciada após o término da fase de alistamento. A fase de apuração é iniciada após o término da fase de votação para garantir o requisito de privacidade (capítulo 5.2).

5.2 Requisitos de segurança

Conforme exposto em [RIE99], um sistema de votação digital deve atender os seguintes requisitos de segurança:

- **Exatidão:** um sistema de votação é exato se (i) não é possível alterar uma cédula,

(ii) toda cédula válida é contada na fase de apuração, e (iii) nenhuma cédula inválida é contada na apuração.

Existem duas possibilidade de exatidão: total e parcial. Na exatidão total, o resultado da apuração é exato, ou porque não é possível haver inconsistências ou porque todas as inconsistências podem ser detectadas e corrigidas. Na exatidão parcial, é possível detectar mas não necessariamente corrigir as inconsistências. A exatidão pode ser medida considerando-se a margem de erro, a probabilidade de erro e o número de pontos em que um erro pode ser introduzido [CC96].

- **Democracia:** um sistema de votação é democrático se (i) apenas votantes autorizados podem participar da votação e (ii) cada votante pode votar uma única vez.

  Este requisito está relacionado à integridade da lista de eleitores. No entanto, são necessárias considerações adicionais para garantir que o administrador da lista de eleitores não viole este requisito.

- **Privacidade:** um sistema de votação garante privacidade se (i) não é possível associar uma cédula ao eleitor que a depositou (anonimato), (ii) nenhum votante pode provar qual foi seu voto (não-coação), e (iii) todos os votos permanecem em segredo até o fim da eleição (imparcialidade).

- **Verificabilidade:** há duas definições para verificabilidade: verificabilidade universal e verificabilidade individual. Um sistema de votação é universalmente verificável se qualquer entidade pode independentemente verificar que todas as cédulas foram contadas corretamente. Por outro lado, um sistema individualmente verificável permite que cada votante verifique que sua cédula foi contada corretamente.

5.3 Requisitos de implementação

Além do interesse teórico no projeto de um sistema de votação digital, caso o objetivo seja a implementação e execução de tal sistema em larga escala é necessário que sejam identificados outros requisitos além dos de segurança. Conforme exposto em [CC96] e [RIE99], pode-se enumerar os seguintes requisitos de implementação:

- **Conveniência:** um sistema de votação digital é conveniente se ele permite que os votantes emitam seus votos de forma rápida, em uma única sessão, com equipamento mínimo e sem a necessidade de habilidades especiais.

  Os votantes devem conseguir votar a partir de seus computadores pessoais onde estará instalado o software de votação bem como as bibliotecas criptográficas. É desejável que também seja possível votar a partir de dispositivos móveis, como telefones celulares. O protocolo de votação não deve envolver computações muito intensivas ou uma grande carga na rede. A usabilidade do software também deve ser levada em consideração.

- **Flexibilidade:** Um sistema de votação digital é flexível se permite vários tipos de opções, incluindo perguntas abertas.

  Apesar de a maioria dos sistemas de votação permitir diversas estratégias de voto, alguns sistemas [BEN87] estão restritos a votos do tipo "Sim/Não" e conseqüentemente não atendem completamente o requisito de flexibilidade.

- **Mobilidade:** um sistema de votação digital é móvel se não há restrições com relação ao local em que o eleitor emite seu voto, considerando-se as restrições impostas pela rede. Um sistema de votação digital que obrigue que os votantes dirijam-se a determinados locais físicos é similar à votação através de urna eletrônica (conforme modelo utilizado no Brasil) no tocante a este requisito.

- **Escalabilidade:** um sistema de votação digital é escalável se ele permite que haja um número indefinido de participantes em uma votação.

Muitos sistemas de votação digital pressupõem a existência de um único centro de votação, limitando portanto a execução da votação em larga escala. O armazenamento das cédulas e a lista de eleitores cresceriam a dimensões não-gerenciáveis, e o próprio centro de votação tornar-se-ia um gargalo. Conseqüentemente, para atender o requisito de escalabilidade, um sistema de votação digital precisa considerar a existência de múltiplos centros de votação.

5.4 Classificação dos sistemas de votação digital

A primeira proposta de um sistema seguro para votação digital foi feita por David Chaum em 1981 [CHA81], como parte de um trabalho sobre comunicação anônima. Desde então, uma série de propostas têm aparecido, geralmente considerando que os participantes são um conjunto de votantes e um conjunto de autoridades de votação. Algumas propostas consideram uma única autoridade de votação, enquanto que outras dividem a funcionalidade da votação entre várias autoridades de votação, cada qual com uma tarefa diferente. Há também propostas em que não há autoridades de votação – o processo de votação é baseado em computações multipartidas seguras –, porém devido ao custo proibitivo possuem apenas interesse teórico [RIE99].

Conforme [RIE99], um princípio básico para a classificação de sistemas de votação digital é a forma como o requisito de segurança de anonimato é solucionado. Há dois grupos principais: os sistemas baseados em misturadores e os sistemas baseados em homomorfismos.

5.4.1 Sistemas baseados em misturadores

Nestes sistemas utiliza-se um canal anônimo entre os votantes e o centro de votação. Usualmente os canais anônimos são implementados através de redes de misturadores, e portanto tais sistemas são ditos baseados em misturadores.

Ao se utilizar um canal de comunicação anônima, o processo de votação é feito em duas fases. Na primeira fase, cada votante é autenticado e recebe uma autorização

para votar. Na segunda fase, o votante utiliza esta autorização para efetivamente votar de forma anônima.

Para evitar que o centro de votação consiga relacionar uma autorização ao votante que a solicitou, é necessário algum mecanismo baseado em criptografia. Os sistemas de votação baseados em misturadores podem ser diferenciados com relação à forma como as autorizações de voto são construídas e emitidas:

- A primeira alternativa, utilizada em [CHA81], consiste em dividir o centro de votação em duas autoridades: uma responsável por emitir as autorizações e outra responsável por receber as cédulas dos votantes. Todavia, se as duas autoridades conspirarem, perde-se o anonimato. Apesar da simplicidade, a segurança deste modelo é questionável.

- A segunda alternativa (uma proposta representativa pode ser encontrada em [SK95]) trabalha de forma oposta à alternativa anterior. Ao invés de o votante obter uma autorização, o centro de votação cria um par criptografado de votos opostos (estes sistemas permitem apenas votos "Sim/Não") em ordem aleatória. A ordem é informada ao votante através de um canal privado, o que acarreta pressuposições físicas (existência de uma linha dedicada e segura entre o local de votação e o centro de votação) que não são práticas.

- A terceira alternativa, representada por [NSS91], é baseada no protocolo de divulgação de segredos tudo-ou-nada (ANDOS – *All-or-Nothing Disclosure of Secrets*). Todavia, a complexidade do protocolo ANDOS é muito maior do que a técnica utilizada na quarta alternativa, e os benefícios são exatamente os mesmos.

- A quarta alternativa, representada por [FOO92], emite as autorizações de votação por intermédio de assinaturas cegas. Excetuando-se a necessidade de utilizar a técnica *cut-and-choose*, a complexidade de uma assinatura cega é igual à de uma assinatura digital comum. Conseqüentemente, assinaturas cegas são geralmente a forma mais aceita de se obter anonimato e democracia em sistemas de votação baseados em misturadores.

5.4.2 Sistemas baseados em homomorfismos

A primeira proposta para esta categoria de sistemas de votação foi feita por Benaloh e Yun em [BY86]. A funcionalidade da votação é distribuída entre várias entidades diferentes, as quais não podem individualmente determinar o voto de um indivíduo. Ademais, se ao menos uma entidade for honesta, uma conspiração entre as demais entidades não conseguirá quebrar o requisito de privacidade; e também obtém-se exatidão total e verificabilidade universal.

Este tipo de sistemas envolve inúmeras técnicas criptográficas, e tem uma natureza bastante complexa. A necessidade de comunicação e processamento para se emitir um voto é grande se comparada aos sistemas baseados em misturadores. A proposta inicial restringia-se a votos do tipo "Sim/Não" e, apesar de alguns avanços, não é possível lidar com perguntas abertas, como por exemplo perguntas onde o indivíduo que responde pode utilizar texto livre em sua resposta.

5.5 Exemplo de Modelos de Votação Digital

Para melhor apresentar a problemática de um modelo de votação digital, serão exemplificados alguns modelos de votação com progressivo aumento de complexidade.

Para o correto entendimento dos modelos de votação e interpretação inequívoca de termos, segue um glossário com as definições mais importantes utilizadas nesta discussão:

- AV: Autoridade de Votação; autoridade responsável por tarefas referentes à votação
- $E_K(M)$: informação M criptografada com a chave K
- KR_A: chave privada da entidade A
- KU_A: chave pública da entidade A
- $Mallory$: atacante que procura burlar o protocolo de votação
- $S_A(M)$: informação M assinada com a chave privada da entidade A

- V: Vera, uma determinada votante
- $voto$: seqüência de bytes representando o voto de V

5.5.1 Modelo Simplista Número 1 [SCH96]

1. V criptografa $voto$ com KU_{AV}
2. V envia $voto$ para AV
3. AV descriptografa os votos com KR_{AV} e publica os resultados.

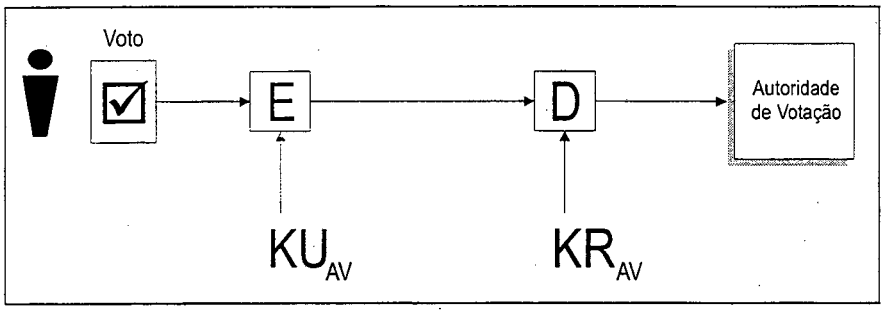

Figura 5.2: Passos do modelo simplista número 1

Este modelo, representado na figura 5.2, possui dois grandes problemas: a não-identificação dos votantes e a possibilidade de um votante enviar mais de um voto.

5.5.2 Modelo Simplista Número 2 [SCH96]

1. V criptografa $voto$ com KR_V, obtendo o voto assinado $S_V(voto)$
2. V criptografa $S_V(voto)$ com KU_{AV}
3. V envia $E_{KU_{AV}}(S_V(voto))$ para AV
4. AV descriptografa os votos, verifica as assinaturas, computa e publica os resultados.

Apesar de este modelo (representado na figura 5.3)resolver os problemas apresentados em 5.5.1, ele não atende o requisito de privacidade. Como cada votante

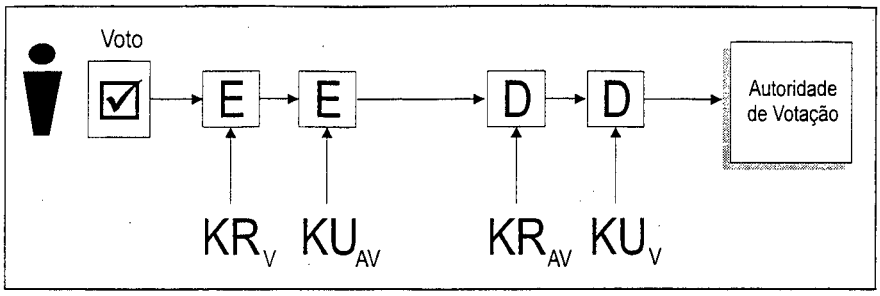

Figura 5.3: Passos do modelo simplista número 2

assina seu voto com sua chave privada, a Autoridade de Votação consegue relacionar o voto ao votante. Para que este modelo possa ser implementado, é necessário que todos os votantes confiem totalmente na honestidade da Autoridade de Votação.

5.5.3 Modelo com Assinaturas Cegas [SCH96]

1. V gera dez conjuntos de mensagens, sendo que cada conjunto contém cada voto possível (por exemplo, se é uma pergunta cujas respostas são "Sim" ou "Não", cada conjunto contém dois votos, um contendo "Sim" e outro contendo "Não"). Além disso, cada mensagem contém um número de identificação gerado aleatoriamente, grande o suficiente para evitar duplicatas com outros votantes

2. V assina cegamente todas as mensagens

3. V envia todas as mensagens, juntamente com os respectivos fatores de ocultação, para AV

4. AV verifica seu banco de dados para garantir que V ainda não tenha votado. São abertos nove dos dez conjuntos de mensagens para verificar que são votos bem formados (ou seja, tem-se probabilidade 0.9 que V tenha submetido votos e não outra informação). O nome de V é armazenado no banco de dados

5. AV assina individualmente todas as mensagens e as envia para V

6. V cancela a ocultação das mensagens, ficando com um conjunto de votos assinados por AV

7. V escolhe um dos votos e o criptografa com KU_{AV}

8. V envia o voto escolhido para AV

9. AV descriptografa os votos, verifica as assinaturas, verifica o banco de dados por números de identificação duplicados, e calcula os resultados. Ao publicar os resultados, para cada voto está relacionado o número serial a ele associado.

Este modelo, representado na figura 5.4, oferece as seguintes garantias:

- Se $Mallory$ tentar enviar o mesmo voto mais de uma vez, AV detecta a duplicidade do número serial (passo 9) e descarta o voto
- Se $Mallory$ tentar enviar mais de um voto, AV detecta que $Mallory$ já votou (passo 4)
- $Mallory$ não pode gerar votos por si próprio porque não possui KR_{AV}, que assina os votos válidos. Pelo mesmo motivo não é possível interceptar e modificar votos de outras pessoas
- AV não consegue determinar qual o voto de V devido ao uso de assinaturas cegas
- Se AV publicar todos os números seriais dos votos que foram apurados, cada votante pode verificar que seu voto foi levado em conta na apuração.

Por outro lado, este modelo apresenta as seguintes falhas:

- Se o passo 8 não for feito de forma anônima, AV pode registrar quem enviou qual voto, e conseqüentemente determinar o voto de cada votante
- AV pode gerar uma série de votos válidos, assinados por ela mesma, e considerá-los na fase de apuração
- Se V descobrir que AV alterou seu voto, não há maneira de prová-lo.

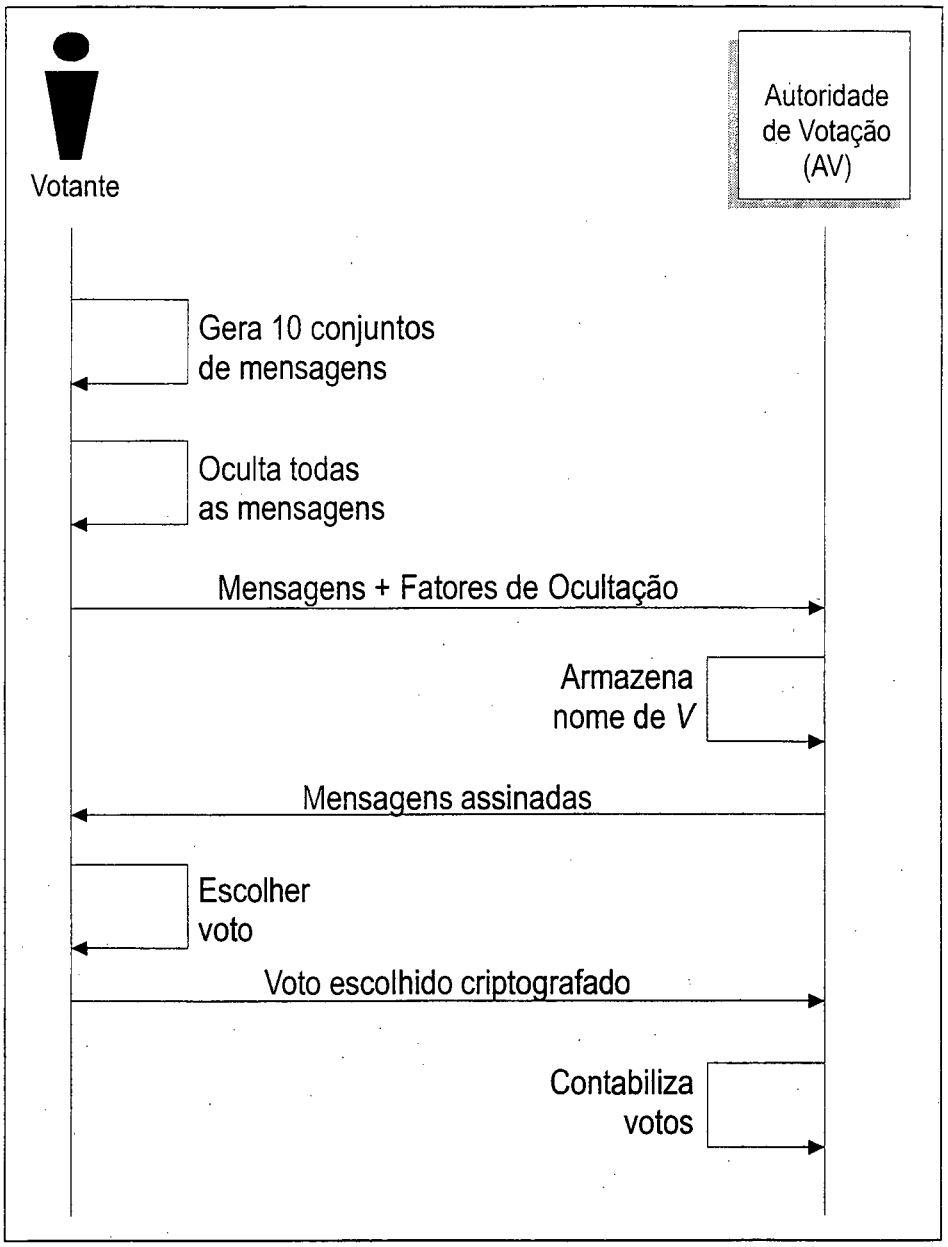

Figura 5.4: Modelo com assinaturas cegas

Capítulo 6

Farnel

Um sistema computacional que permita a execução de votações digitais na Internet de forma segura deve conter um protocolo criptográfico específico e uma arquitetura de implementação apropriada. Neste capítulo é apresentado o protocolo Farnel, uma proposta de protocolo criptográfico para votação digital. Uma das características deste protocolo é o objetivo de tentar, na medida do possível, mimetizar os procedimentos de votação no Brasil antes do advento da urna eletrônica. Tais procedimentos são de conhecimento geral da população, e por conseguinte quaisquer analogias tornam-no de mais fácil compreensão, possivelmente gerando um sentimento maior de confiança em relação ao protocolo.

O protocolo Farnel foi especificado com base em um ambiente isento de falhas ou faltas i.e. todos os componentes computacionais estão corretos e sempre disponíveis. Neste ambiente ideal não há problemas de perda do canal de comunicação ou dos dados envolvidos, o que possibilita concentrar-se nos requisitos de segurança que são o foco deste trabalho.

6.1 Protocolo Farnel

O protocolo Farnel é essencialmente um protocolo para a fase de votação. Não obstante, há um conjunto de tarefas que devem ser executadas antes e depois da votação para que

o sistema de votação digital como um todo seja executado de forma correta e segura. O protocolo Farnel será apresentado, bem como os procedimentos específicos a cada fase no processo de votação digital, de acordo com a notação a seguir.

6.1.1 Notação

Para permitir o entendimento inequívoco do protocolo, a seguinte notação é utilizada para descrever os participantes, mensagens e ferramentas criptográficas:

AV: autoridade de votação; responsável por tarefas relacionadas à votação

AA: autoridade de alistamento, responsável por emitir os certificados de autorização para votar

AE: autoridade de escrutínio, responsável por garantir o trabalho honesto da autoridade de votação

S: conjunto das autoridades de escrutínio

KR_A: chave privada de A

KU_A: chave pública de A

$H(M)$: resumo (*hash*) da mensagem M

$B_k(M)$: mensagem M ocultada pelo fator k

$S_A(M)$: mensagem M assinada com a chave privada de A; contém a mensagem (M) e a assinatura em si ($s_A(M)$)

$BS_A(M_k)$: mensagem M, ocultada pelo fator k, assinada cegamente com a chave privada de A; contém a mensagem (M_k) e a assinatura em si ($bs_A(M_k)$)

$MS_{\mathcal{X}}(M)$: mensagem M assinada com as chaves privadas de todos os elementos pertencentes a $\mathcal{X}$; contém a mensagem (M) e a assinatura em si ($ms_{\mathcal{X}}(M)$)

$MBS_{\mathcal{X}}(M_k)$: mensagem M, ocultada pelo fator k, assinada cegamente com as chaves privadas de todos os elementos de $\mathcal{X}$; contém a mensagem (M_k) e a assinatura em si ($mbs_{\mathcal{X}}(M_k)$)

V: Victor, um votante

voto: seqüência de bytes representando um voto

cedula: seqüência de bytes representando uma cédula

LV: lista de votantes

$\#X$: número de elementos no arranjo X

RM: rede de mistura utilizada por V para enviar cédulas a AV de forma anônima

$\mathcal{A}$: arranjo de cédulas assinadas pelas autoridades de escrutínio

$\mathcal{A}_0$: arranjo inicial de cédulas contendo todas as possíveis combinações de votos, contendo k cópias de uma mesma cédula

$\mathcal{B}$: arranjo de cédulas assinadas pelos votantes

$RM_{\mathcal{A}}$: rede de mistura para o arranjo $\mathcal{A}$; eventualmente chamada de "urna"

$\mathcal{C}$: arranjo com todas as cédulas possíveis

$\mathcal{F}$: arranjo final de votos que devem ser apurados

`idvotacao`: número que identifica a votação

`id-idvotacao`: OID referente a `idvotacao`

DIR: diretório da votação; local onde estão armazenadas informações referentes a uma determinada votação

$A \rightarrow B : M$: A envia a mensagem M para B

6.1.2 Fase de configuração

Nesta fase é gerado o par de chaves da autoridade de votação AV e é emitido um certificado digital padrão X.509 v3[1]. O certificado contém uma extensão crítica informando o número que identifica a votação (`idvotacao`). O certificado é tornado público através do diretório DIR para que todas as entidades tenham ciência da chave pública da autoridade de votação (KU_{AV}).

A extensão contendo `idvotacao` é definida em ASN.1 [ITU97b] da seguinte forma:

```
id-idvotacao OBJECT-IDENTIFIER ::= { iso(1) org(3)
dod(6) internet(1) private(4) enterprise(1)
ufsc/labsec(7687) ostracon(1) idvotacao(1) }

idvotacao ATTRIBUTE ::= { WITH SYNTAX INTEGER
ID id-idvotacao }
```

O conjunto S de autoridades de escrutínio também é definido de forma a garantir a honestidade da autoridade de votação AV. Para cada autoridade de escrutínio é gerado um par de chaves e emitido um certificado digital correspondente, publicado em DIR.

Além disso, após a definição das opções de votação, AV gera o arranjo C composto por todas as possíveis combinações de opções de voto. O fato de o arranjo C ter sido gerado com todas as possíveis cédulas evita que, durante a fase de votação (em que ao entrar uma cédula na urna outra é retirada), seja possível saber qual a cédula inserida pelo votante (se todas as possíveis cédulas estão na urna, então há ao menos uma cédula na urna que é igual à cédula do votante. Por outro lado, se apenas um sub-arranjo das cédulas disponíveis está na urna, existe a possibilidade de a cédula do votante não pertencer a este sub-arranjo e ser retirada logo em seguida da urna, quebrando portanto o requisito de privacidade). Após a verificação, C é assinado pelas autoridades de escrutínio S e é publicado em DIR.

[1]No decorrer deste texto os termos "certificado digital" e "certificado digital padrão X.509 v3" são intercambiáveis.

6.1.3 Fase de alistamento

Nesta fase os votantes precisam autenticar-se perante a autoridade de alistamento AA (e.g. através de documentos de identidade ou certificados digitais), sendo aprovados como documentos de autenticação para votação específica de acordo com critérios estabelecidos pela autoridade de alistamento. Todos os votantes autorizados recebem um número de identificação definido por `idvotante` e são incluídos na lista de votantes LV, a qual é publicada no diretório DIR. Sendo o diretório público, as autoridades de escrutínio, os votantes ou quaisquer entidades podem verificar a correta formação desta lista[2].

A extensão do número identificador do votante e a lista de votantes podem ser definidas em ASN.1 como:

```
id-idvotante OBJECT-IDENTIFIER ::= { iso(1) org(3)
dod(6) internet(1) private(4) enterprise(1)
ufsc/labsec(7687) ostracon(1) idvotante(2) }

idvotante ATTRIBUTE ::= { WITH SYNTAX INTEGER
ID id-idvotante }

RegistroVotante ::= SEQUENCE { idvotante, nome =
IA5String, certificado = BIT STRING }

LV ::= SEQUENCE { idvotacao, votantes = SET OF
RegistroVotante }
```

Algumas possibilidades de autenticação do votante perante a autoridade de alistamento AA podem ser vislumbradas:

- Traçando-se um paralelo com o atual sistema de identificação utilizado nas eleições oficiais para cargos públicos, a autoridade de alistamento emitiria certificados digitais (títulos eleitorais digitais) análogos aos títulos de eleitor. Caso o eleitor

[2]Presume-se que, após a publicação da lista de votantes, haja um prazo hábil para que quaisquer anomalias que porventura existam possam ser identificadas e corrigidas.

ainda não tenha o título eleitoral digital, a autoridade de alistamento emite-o. Cada eleitor é inserido na lista de votantes com o seu título eleitoral digital correspondente.

- Outra possibilidade é a autoridade de alistamento, após identificar o votante, emitir um certificado digital específico para a votação em questão (este certificado assemelha-se aos certificados de atributo atualmente em fase de definição[3] pela IETF [IETF01]). O certificado conteria a extensão `idvotacao` indicando a que votação o votante está autorizado. Desta forma, a autoridade de alistamento poderia utilizar quaisquer métodos de autenticação que fossem convenientes, e sempre haveria um certificado digital específico para aquela votação. Conseqüentemente, o processo de autenticação durante a fase de votação pode ser feito com base nas propriedades deste certificado.

- A autoridade de alistamento também poderia definir quais os certificados digitais aceitáveis como meios de autenticação dos votantes. Estes certificados teriam como emissor alguma autoridade certificadora na qual a autoridade de alistamento depositaria confiança. Este é, por exemplo, o mecanismo adotado por navegadores Web quando da validação de um certificado digital de autenticação de um servidor Web. Todavia, para correção do protocolo, este certificado precisa conter a extensão `id-idvotante`.

Independentemente do método utilizado, o resultado final é uma lista de votantes em que o registro de cada votante contém o número identificador do votante e uma representação binária do certificado digital que deve necessariamente ser utilizado pelo votante durante a fase de votação.

Com relação ao Farnel, esta fase tem uma tarefa importante: a criação do arranjo inicial de cédulas

$$\mathcal{A}_0 = \{c_1, c_2, \ldots, c_k | \forall c \in \mathcal{C}, k \in \mathbb{N}, k \cdot \#\mathcal{C} \geqslant \#LV\}.$$

[3] *Internet Engineering Task Force.*

Esta criação é feita da seguinte forma: define-se um valor k tal que o número de cédulas disponíveis no arranjo $\mathcal{A}_0$ seja maior ou igual ao número de votantes na lista de votantes LV, ou seja, $\#AV = k \cdot \#\mathcal{C} \geqslant \#LV$. As cédulas inicialmente disponíveis são obtidas por meio da criação de, para cada cédula possível em $\mathcal{C}$, k cédulas idênticas no arranjo $\mathcal{A}_0$. Este arranjo é assinado por $\mathcal{S}$, publicado em DIR, e depositado na rede de mistura $RM_{\mathcal{A}}$.

Conjetura: quanto maior o valor de k, maior o número de cédulas contidas em $\mathcal{A}_0$ e por conseguinte diminui-se a probabilidade de, em uma escolha aleatória, obter-se a cédula mais votada.

6.1.4 Fase de votação

É na fase de votação que está o cerne do protocolo Farnel. Para facilitar o entendimento desta fase, o protocolo foi dividido em três etapas: autenticação mútua, obtenção da cédula em branco e emissão da cédula preenchida.

6.1.4.1 Etapa de autenticação mútua

Nesta etapa é necessário que cada votante V identifique-se perante a autoridade de votação AV por meio do seu número de identificação (`idvotante`) e do certificado digital que foi registrado na lista de votantes durante a fase de alistamento. Em contrapartida, o votante precisa ter certeza de que está realmente em contato com a autoridade de votação correta. Esta autenticação mútua pode ser feita através do protocolo SSL com a verificação da autoridade certificadora que emitiu o certificado de AV e a extensão `idvotacao` contida neste certificado. Após a autenticação, é criado um canal de comunicação com os serviços de confidencialidade, identificação, integridade e não-repúdio.

6.1.4.2 Etapa de obtenção de cédula em branco

A cédula em branco é gerada pela autoridade de votação AV e deve conter todas as opções de voto. As autoridades de escrutínio $\mathcal{S}$ verificam se a cédula está corretamente formada

e a assinam, gerando $MS_{\mathcal{S}}(cedula_b)$, e posteriormente enviam-na para AV, que por sua vez repassa-a para V.

Quando o votante V recebe a cédula em branco $MS_{\mathcal{S}}(cedula_b)$, ele verifica a assinatura $ms_{\mathcal{S}}(cedula_b)$ por meio da chave pública das autoridades de escrutínio. Se a assinatura não for válida, o protocolo é encerrado. Se a assinatura for válida, V remove a assinatura e obtém a cédula em branco $cedula_b$.

1. AV gera $cedula_b$
2. $AV \rightarrow \mathcal{S} : cedula_b$
3. $\mathcal{S}$ gera $MS_{\mathcal{S}}(cedula_b)$
4. $\mathcal{S} \rightarrow AV : MS_{\mathcal{S}}(cedula_b)$
5. $AV \rightarrow V : MS_{\mathcal{S}}(cedula_b)$
6. V verifica $MS_{\mathcal{S}}(cedula_b)$; gera $cedula_b$

6.1.4.3 Etapa de emissão da cédula com os votos

De posse de $cedula_b$, o votante a assina gerando $s_V(cedula_b)$. A assinatura da cédula em branco será enviada posteriormente à autoridade de votação para comprovar que o votante recebeu uma cédula em branco e entregou uma cédula preenchida (passo 1).

O votante então preenche seus votos escolhendo as opções contidas na cédula, gerando a cédula preenchida $cedula_p$. Em seguida o votante escolhe aleatoriamente um fator de ocultação k e cega a cédula $cedula_p$ com este fator, gerando $B_k(cedula_p)$ (passo 2).

É criado pelo votante um envelope E tal que $E =$ `idvotante` $||$ $s_V(cedula_b)$ $||$ $B_k(cedula_p)$. Este envelope é assinado pelo votante, gerando $S_V(E)$, e é encaminhado para a autoridade de votação. AV repassa o envelope às autoridades de escrutínio (passos 3 a 6).

Ao receber o envelope, cada autoridade de escrutínio verifica se a assinatura do votante corresponde ao certificado digital equivalente à entrada na lista de votantes LV

identificada por `idvotante`. Em caso afirmativo, a autoridade de escrutínio registra em sua lista particular de votantes que o votante entregou a cédula preenchida e procede à assinatura cega da cédula preenchida pelo votante ($MBS_{\mathcal{S}}(cedula_p)$). Após todas as autoridades de escrutínio assinarem cegamente a cédula preenchida, ela é repassada à autoridade de votação que por sua vez envia-a para o votante (passos 7 a 11).

De posse da cédula preenchida assinada pelas autoridades de escrutínio $MBS_{\mathcal{S}}(cedula_p)$, o votante remove a ocultação e obtém a assinatura da cédula preenchida $ms_{\mathcal{S}}(cedula_p)$. Esta cédula é então enviada à rede de mistura $RM_{\mathcal{A}}$ juntamente com a identificação do votante (passos 12 a 14).

A rede de mistura $RM_{\mathcal{A}}$, ao receber a cédula do votante, verifica com todas as autoridades de escrutínio se o votante já depositou uma cédula antes. Caso a rede de mistura receba uma resposta negativa de todas as autoridades de escrutínio, ou seja, é a primeira vez que o votante está depositando uma cédula, a cédula é aceita. A rede de mistura gera um recibo de entrega de cédula contendo a identificação da votação e a identificação do votante $recibo =$ `idvotacao` $||$ `idvotante` e solicita às autoridades de escrutínio que o assinem, gerando $MS_{\mathcal{S}}(recibo)$. Este recibo é entregue ao votante (passos 15 a 21).

1. V gera $s_V(cedula_b)$
2. V gera $B_k(cedula_p)$
3. V gera $E =$ `idvotante` $|| s_V(cedula_b) || B_k(cedula_p)$
4. V gera $S_V(E)$
5. $V \rightarrow AV : S_V(E)$
6. $AV \rightarrow \mathcal{S} : S_V(E)$
7. $\mathcal{S}$ verifica $S_V(E)$
8. $\mathcal{S}$ assinala entrega de cédula de V
9. $\mathcal{S}$ gera $MBS_{\mathcal{S}}(cedula_p)$

10. $\mathcal{S} \rightarrow AV : MBS_{\mathcal{S}}(cedula_p)$

11. $AV \rightarrow V : MBS_{\mathcal{S}}(cedula_p)$

12. V verifica $MBS_{\mathcal{S}}(cedula_p)$

13. V gera $MS_{\mathcal{S}}(cedula_p)$

14. $V \rightarrow RM_{\mathcal{A}} : MS_{\mathcal{S}}(cedula_p), \texttt{idvotante}$

15. $RM_{\mathcal{A}}$ verifica se votante já depositou alguma cédula

16. $RM_{\mathcal{A}}$ deposita $MS_{\mathcal{S}}(cedula_p)$

17. $RM_{\mathcal{A}}$ gera $recibo$

18. $RM_{\mathcal{A}} \rightarrow \mathcal{S} : recibo$

19. $\mathcal{S}$ gera $MS_{\mathcal{S}}(recibo)$

20. $\mathcal{S} \rightarrow RM_{\mathcal{A}} : MS_{\mathcal{S}}(recibo)$

21. $RM_{\mathcal{A}} \rightarrow V : MS_{\mathcal{S}}(recibo)$

6.1.5 Fase de encerramento da votação

As autoridades de escrutínio solicitam o esvaziamento da rede de mistura $RM_{\mathcal{A}}$ e assinam o arranjo $\mathcal{A}$ resultante. A partir deste momento, nenhuma cédula pode ser inserida no arranjo $\mathcal{A}$.

As cédulas constantes no arranjos $\mathcal{A}$ são publicadas no diretório DIR.

6.1.6 Fase de apuração

O arranjo final de votos a serem apurados, denominado $\mathcal{F}$, é dado por $\mathcal{F} = \mathcal{A} - \mathcal{A}_0$. O arranjo $\mathcal{F}$ é publicado em DIR, bem como o resultado da votação em formato apropriado à característica da votação.

Como o arranjo $\mathcal{A}_0$ foi publicado em DIR na fase de alistamento, e os arranjos $\mathcal{A}$ e $\mathcal{F}$ foram publicados na fase de encerramento de votação, qualquer entidade pode efetuar a conferência da exatidão da apuração.

6.2 Análise dos requisitos de segurança

6.2.1 Definições

Honestidade das autoridades de escrutínio: o Farnel parte do princípio de que ao menos uma das autoridades de escrutínio é honesta, de tal forma que qualquer corrupção que poderia ser feita pela autoridade de votação AV seja detectada por alguma autoridade de escrutínio AE.

Honestidade da rede de mistura: de acordo com [CHA81], por definição uma rede de mistura é honesta se ao menos um dos servidores que compõem a rede de mistura é honesto.

6.2.2 Requisito de Exatidão

O requisito de exatidão pode ser dividido nos seguintes itens:

- **Não é possível alterar uma cédula.** As cédulas inseridas na rede de mistura $RM_{\mathcal{A}}$ são previamente assinadas pelas autoridades de escrutínio $\mathcal{S}$, garantindo que qualquer alteração em uma cédula possa ser detectada. Neste caso a cédula não é considerada válida.

- **Toda cédula válida é contada na fase de apuração.** Como os votantes encaminham suas cédulas à rede de mistura $RM_{\mathcal{A}}$, pressupõe-se que o arranjo $\mathcal{A}$ contenha todas as cédulas válidas. Neste caso a apuração é exata desde que o componente computacional que faça a apuração seja correto. A exatidão da apuração está diretamente ligada à exatidão da verificação: se o componente responsável pela apuração falhar por algum motivo é possível que entidades independentes consigam verificar esta falha na contagem.

- **Nenhuma cédula inválida é contada na apuração.** Analogamente ao item anterior, a correção do componente computacional é fator a ser considerado, e a possibilidade de verificação da apuração resolve a confiança na exatidão da apuração. Quaisquer cédulas inválidas que porventura tenham sido inseridas em $RM_{\mathcal{A}}$ não terão a assinatura das autoridades de escrutínio, e conseqüentemente não podem ser consideradas na apuração. Além disso, cédulas que originalmente tenham sido válidas mas foram alteradas em algum momento causam a não-validade da assinatura das autoridades de escrutínio, e conseqüentemente são consideradas inválidas.

6.2.3 Requisito de Democracia

O requisito de democracia pode ser dividido nos seguintes itens:

- **Apenas votantes autorizados podem participar da votação.** Para o votante receber uma cédula em branco válida é necessário que ele se autentique perante AV e receba uma cédula em branco assinada por $\mathcal{S}$. Para que um votante consiga depositar a cédula na rede de mistura $RM_{\mathcal{A}}$ é necessário que ele se identifique através de seu número de identificação e de uma assinatura com sua chave privada, a qual é contrastada com a chave pública presente no certificado digital que está na lista de votantes autorizados durante a fase de alistamento. Desta forma, votantes que não estejam presentes na lista de votantes não conseguirão depositar cédulas na rede de mistura $RM_{\mathcal{A}}$.

- **Cada votante pode votar uma única vez.** A rede de mistura $RM_{\mathcal{A}}$, antes de aceitar uma cédula preenchida, verifica com todas as autoridades de escrutínio se o votante autenticado já não depositou uma cédula antes. Caso alguma autoridade de escrutínio indique que o votante já entregou uma cédula, ele é impedido de entregar quaisquer outras cédulas. Como por definição ao menos uma autoridade de escrutínio é honesta, impede-se que um votante consiga votar mais de uma vez.

6.2.4 Requisito de Privacidade

O requisito de privacidade pode ser dividido nos seguintes itens:

- **Anonimato: Não é possível associar uma cédula ao eleitor que a depositou.** Como a cédula preenchida pelo votante é inserida na rede de mistura $RM_{\mathcal{A}}$, e por definição a rede mistura é honesta, o rastreamento entre votante e cédula não é exeqüível. Além disso, a cédula em branco que o votante recebe para poder gerar a cédula preenchida com seus votos não contém nenhuma identificação que permita o rastreamento do votante.

- **Nenhum votante pode provar qual foi seu voto.** Como a cédula preenchida pelo votante é inserida na rede de mistura $RM_{\mathcal{A}}$, não é possível estabelecer a ligação entre votante e cédula. Ademais, a cédula que o votante assina com sua chave privada é uma cédula aleatória oriunda de $RM_{\mathcal{A}}$. Por conseguinte, o votante não consegue provar qual foi a cédula que ele preencheu. Observa-se que o votante detém em seu poder duas cédulas assinadas pelas autoridades de escrutínio: a sua própria cédula, por ele preenchida, e outra cédula que foi-lhe enviada por $RM_{\mathcal{A}}$. Estas duas cédulas são indistinguíveis. Nenhuma delas pode ser utilizada como prova dos votos do votante porque elas também são idênticas a todas as outras cédulas.

- **Imparcialidade: Todos os votos permanecem em segredo até o fim da votação.** As cédulas permanecem na rede de mistura criptografadas com as chaves públicas de cada servidor que compõem a rede de mistura. Enquanto a rede de mistura não for instruída a esvaziar todo o seu conteúdo garante-se a confidencialidade de todas as cédulas.

6.2.5 Verificabilidade

Considerando-se que todos os arranjos envolvidos na fase de apuração ($\mathcal{A}_0$, $\mathcal{A}$, $\mathcal{F}$), bem como a lista de votantes LV, estão publicados em DIR, qualquer entidade pode usar estes

arranjos para verificar a correta apuração da votação. Obtém-se, portanto, verificabilidade universal.

6.2.6 Conclusão

Pena análise dos requisitos de segurança pode-se concluir que o protocolo Farnel é seguro assumindo-se que as definições de honestidade das autoridades de escrutínio e honestidade da rede de mistura seja garantida.

Capítulo 7

Conclusões

Este trabalho consistiu em uma proposta de protocolo criptográfico para votação digital segura como resultado da pesquisa de mestrado na área de criptografia e segurança em redes de computadores. Fez-se a revisão bibliográfica dos protocolos de votação disponíveis, a qual propiciou o entendimento de quais são os requisitos necessários para um sistema de votação digital, bem como as técnicas comumente utilizadas neste tipo de sistemas. Em particular, ficou caracterizada a separação entre protocolos baseados em homomorfismos e os baseados em canais de comunicação anônima.

Em primeiro lugar, percebeu-se a complexidade característica de sistemas para votação digital. Um sistema desta natureza envolve uma série de considerações: a especificação do protocolo criptográfico em si em relação a requisitos de segurança e implementação, bem como seu comportamento durante as várias fases que constituem o processo de votação; o número de entidades que precisam ser confiáveis para a consecução da votação; a necessidade de infra-estruturas de chave pública confiáveis para lidar com os certificados digitais; o controle da publicação no diretório DIR; a disponibilidade e segurança de cada componente da arquitetura de implementação.

O protocolo Farnel, apresentado nesta dissertação, é um subsistema componente de um sistema de votação digital. Procurando construir analogias com o processo de votação manual utilizado no Brasil antes do advento da urna eletrônica, o protocolo é uma composição ordenada de mecanismos e técnicas criptográficas com o objetivo de

estabelecer regras durante a comunicação entre as entidades participantes de uma votação através da Internet. É utilizada a primitiva de rede de mistura para a funcionalidade de canal anônimo que, em conjunto com a técnica de assinatura cega, garantem a privacidade do voto.

Com relação à implantação em um futuro imediato de sistemas de votação digital para eleições oficiais, há ainda uma série de fatores a serem discutidos. Além das questões técnicas apresentadas no capítulo A, tais como a distribuição das autoridades de votação, a autenticação de código, o gerenciamento de chaves privadas e certificados e a segurança dos componentes computacionais envolvidos, alguns fatores políticos podem ser vislumbrados [HC01], como por exemplo o possível desfavorecimento de grupos sociais que não tenham acesso a computadores e a erosão do "ritual cívico" de deslocar-se fisicamente a uma seção eleitoral para votar. Após as primárias do partido democrata do estado do Arizona (EUA) para preferência presidencial, realizadas entre 7 e 11 de março de 2000 com a possibilidade de votar pela Internet, percebeu-se que [MG01] (i) o fator humano não pode ser subestimado (várias linhas de suporte estavam disponíveis, porém não havia sido previsto que muitos votantes queriam ser os primeiros a votar – ocasionando congestionamento nas primeiras horas em que a votação havia sido iniciada, ou então que vários votantes possuem hábitos noturnos em contraste ao horário comercial) (ii) o requisito de utilização de criptografia forte implicou a necessidade de ter navegadores Web com atualizações recentes, o que não refletia a realidade de todos os votantes; (iii) preocupações com acessibilidade fazem parte de um processo contínuo; (iv) a disponibilização de votação através da Internet em locais físicos pré-determinados (tais como as seções eleitorais) pouco acrescenta ao processo de votação, e aumenta o custo da eleição.

7.1 Trabalhos Futuros

Dada a complexidade de um sistema completo para votação digital segura, pode-se citar vários trabalhos futuros: (i) a formalização e análise do protocolo Farnel utilizando uma técnica de especificação formal ([MEA00], [HP00], [AG97], [MMS97]); (ii) a

especificação detalhada de uma arquitetura de implementação necessária para a efetiva viabilidade do protocolo dentro de um sistema que possa ser utilizado de forma prática; (iii) o estudo da escalabilidade do sistema de votação digital considerando seus componentes arquiteturais e a proposta de organização de hierarquias de autoridades de votação; (iv) o detalhamento do funcionamento de uma rede de mistura de acordo com os pressupostos utilizados (saída automática de uma mensagem a partir de uma entrada, esvaziamento autenticado); (v) a possibilidade de substituir a autoridade de votação AV pelo conjunto das autoridades de escrutínio durante a fase de votação: nesta situação estima-se a utilização de técnicas de computação distribuída segura e criptografia de limiar *(threshold cryptography)* [CGJ+99]; (vi) o estudo de um modelo simplificado para tomadas de decisão, que apesar de funcionalmente serem similares às eleições oficiais, geralmente ocorrem em escopo menor; (vii) a especificação do protocolo levando-se em consideração as características de computação móvel; (viii) a especificação (e talvez a definição de uma linguagem formal) das relações de confiança entre as diversas entidades envolvidas, (ix) a análise do protocolo em relação a requisitos de concorrência. Além disso, o desenvolvimento e implantação de um sistema utilizando o protocolo Farnel para efetuar uma votação digital é uma forma de validar o protocolo do ponto de vista prático.

Apêndice A

Arquitetura de implementação

A arquitetura de um sistema computacional contempla a estrutura do sistema, protocolos de comunicação entre os componentes, funcionalidade de cada componente e distribuição física, entre outros [GS93]. Este apêndice procura discutir tópicos que devem ser levados em consideração na especificação da arquitetura de um sistema de votação digital que utilize o protocolo Farnel. É importante ressaltar que não se objetiva exaurir os tópicos apresentados e sim tecer alguns comentários sobre os aspectos de implementação de um sistema baseado no protocolo Farnel.

A.1 Robustez do protocolo

Conforme exposto no capítulo 6, o protocolo foi definido com base em um ambiente ideal onde as entidades envolvidas no protocolo não apresentam falhas. Um sistema no mundo real, entretanto, apresenta várias possibilidades de falhas durante sua execução. Ademais, neste trabalho não houve preocupação com o controle de concorrência, i.e., vários votantes simultaneamente em contato com a autoridade de votação, as autoridades de escrutínio e a rede de mistura. Por conseguinte, a implementação prática de um sistema de votação digital precisará levar em conta, na especificação do protocolo Farnel, requisitos de tolerância a falhas e controle de concorrência.

A.2 Linguagens de programação

Dentre as possibilidades de linguagens de programação e tecnologias para o desenvolvimento de aplicações que sejam executadas na Internet, pode-se definir as seguintes categorias: (i) Tipo 1: HTML como linguagem de apresentação da interface em navegadores Web, linguagens de script para navegadores (JavaScript ou VBScript) e linguagens para execução no servidor Web (CGIs ou linguagens de script de servidor, tais como PHP ou ASP); (ii) Tipo 2: *plug-ins* para navegadores que utilizem linguagens de programação mais completas, tais como Java *applets*, componentes ActiveX para o navegador Microsoft Internet Explorer ou *plug-ins* em C para o navegador Netscape Navigator; e (iii) Tipo 3: aplicações que prescindam de um navegador Web, podendo ser desenvolvidas em qualquer linguagem de programação que permita conexões através da Internet. Os tipos 1 e 2 são comumente denominados *aplicações Web* devido à utilização de navegadores Web.

A.2.1 Aplicação Internet Tipo 1

Um dos requisitos de privacidade é que o voto emitido pelo votante seja anônimo, ou seja, não deve ser possível relacionar a cédula de voto ao votante que a emitiu. É por este motivo que o votante deve encaminhar sua cédula diretamente à rede de mistura, responsável por garantir o anonimato. Se os procedimentos de assinatura, ocultação e criptografia forem feitos por um servidor Web, ele terá acesso ao conteúdo da cédula e poderá relacioná-la ao votante. Nesta situação, o servidor Web onde estará sendo executada a lógica da aplicação precisa ser extremamente confiável e seguro, o que na prática pode ser difícil de se obter.

Por outro lado, os navegadores Microsoft Internet Explorer, Netscape Navigator e Opera possuem mecanismos internos para gerência de chaves privadas e certificados (o Microsoft Internet Explorer utiliza, de forma integrada, os mecanismos de gerência do sistema operacional Microsoft Windows). As aplicações do tipo 1 poderiam beneficiar-se de tais mecanismos internos e serem executadas de forma integrada com o navegador. No entanto, o Microsoft Internet Explorer não disponibiliza funções criptográficas através de

suas linguagens de script. O Netscape Navigator e o Opera permitem, de forma limitada, apenas o mecanismo de assinatura digital.

A.2.2 Aplicação Internet Tipo 2

Uma solução para o problema citado na seção A.2.1 é o navegador Web efetuar todas as operações criptográficas. Devido às características limitadas de programação disponíveis nos navegadores Web (*JavaScript* ou *VBScript*, as quais são linguagens de programação interpretadas), tais operações ou não podem ser programadas ou exigem um esforço computacional muito grande. A extensão da funcionalidade do navegador através de *plug-ins* permitiria a realização das operações criptográficas necessárias à execução do protocolo Farnel.

Java aparenta ser a linguagem mais apropriada devido à sua característica multiplataforma (aliás, *Java é uma plataforma*) e disponibilidade de bibliotecas criptográficas acessíveis através de uma arquitetura [KNU98]. Além disso, *applets* Java podem ser assinadas digitalmente, garantindo autenticação e integridade do código recebido pelo navegador Web. Todavia, ainda não parece claro qual será o futuro de Java em plataformas Windows devido à recente disputa entre Microsoft e Sun.

A utilização de componentes ActiveX especificamente desenvolvidos para efetuar os passos do protocolo Farnel é uma alternativa interessante porque, assim como *applets* Java, podem ser assinados digitalmente. Além disso, podem acessar os mecanismos criptográficos e de gerência de chaves privadas e certificados do Microsoft Windows, oferecendo portanto uma grande integração com o sistema operacional. Todavia, componentes ActiveX estão limitados ao sistema operacional Microsoft Windows (e talvez ao navegador Microsoft Internet Explorer).

Os *plug-ins* para o Netscape Navigator também não são uma alternativa completa porque são específicos para este navegador. Ademais, o Netscape Navigator não possui uma forma de integração e utilização de seu mecanismo de gerência de chaves privadas e certificados digitais.

A.2.3 Aplicação Internet Tipo 3

Neste tipo de aplicação Internet pode-se utilizar qualquer linguagem de programação que permita estabelecer conexões através da Internet. A interface gráfica não é limitada à disponível em navegadores Web, ampliando-se as possibilidades de interação homem-computador. A integração com os mecanismos implícitos do sistema operacional também é mais direta. Esta foi a solução adotada pela Secretaria da Receita Federal do Ministério da Fazenda para a aplicação de declaração de Imposto de Renda através da Internet.

Uma desvantagem aparente deste tipo de aplicação é a distribuição do código executável. Normalmente a aplicação precisa ser obtida pelo usuário e instalada em seu computador. A atualização de novas versões pode ser feita de forma automática para evitar problemas de versionamento. Além disso é desejável que o usuário possa confiar na aplicação instalada em seu computador, ou seja, que o código nela constante não tenha sido alterado e haja dependências mínimas de outros componentes, como bibliotecas de vínculo dinâmico, as quais poderiam ter sido alteradas de forma indevida.

A.3 Rede de mistura

A rede de mistura utilizada no protocolo Farnel precisa de que haja esvaziamento autenticado, ou seja, a rede somente deve permitir que entidades devidamente autenticadas consigam esvaziar a rede de mistura e verificar seu conteúdo. Pode-se perceber a comparação com uma urna tradicional que pode ser esvaziada para que se tenha acesso às cédulas nela contidas.

A.4 Sintaxe e semântica da cédula de votação

Durante este trabalho tratou-se a cédula (e os votos nela contidos) como uma seqüência de bytes. Isto torna o protocolo versátil porque independe do formato da cédula e dos votos, ou seja, é possível ter perguntas do tipo "Sim/Não", múltipla escolha ou perguntas abertas.

Todavia, para a implementação efetiva de um sistema baseado no Farnel, é necessário especificar a sintaxe e a semântica da cédula, possivelmente em alguma notação de descrição e continência de dados como ASN.1 ou XML.

A.5 Identificação dos votantes

Cada votante deverá ter um certificado digital padrão X.509v3 reconhecido pela autoridade de votação. Em uma eleição oficial para cargos públicos no Brasil, este certificado é análogo ao título de eleitor – neste caso, o Tribunal Superior Eleitoral estaria encarregado de definir de que forma um determinado certificado X.509v3 é válido como título de eleitor. Esta definição poderia ser feita através do emissor do certificado (a autoridade certificadora que emitiu o certificado pertenceria à infra-estrutura de chave pública do TSE ou seria credenciada pelo tribunal), e também pela definição de extensões no próprio certificado.

O censo eleitoral, ou seja, a lista de votantes autorizados será publicada em um serviço de diretório distribuído (X.500 ou LDAP). A distribuição do diretório é irrelevante para pequenos grupos (como os moradores de um condomínio), porém quando se considera uma eleição nacional (como as eleições para Presidente da República no Brasil) torna-se bastante claro que um único servidor contendo o diretório de todos os eleitores é um gargalo que precisa ser reduzido. Um diretório distribuído aumenta a escalabilidade do sistema por meio da distribuição da carga entre múltiplos servidores.

A.6 Distribuição das autoridades de votação

Assim como o censo eleitoral é disponibilizado por meio de um diretório distribuído, faz sentido que a responsabilidade da autoridade de votação também seja distribuída para evitar gargalos no sistema de votação digital. O conceito de *árvore de votação* [RBR97] organiza uma árvore de autoridades de votação da seguinte maneira: o nó raiz representa a ANV (Autoridade Nacional de Votação), a qual equivaleria ao Tribunal Superior Eleitoral em uma comparação com a organização das eleições públicas no Brasil. Abaixo da ANV

podem existir CEs (Colégios Eleitorais) e CCs (Centros de Contagem). O CE representa a AV à qual um votante está relacionado e com quem ele se comunica para efetuar seu voto; pode ser comparado a uma zona eleitoral. Para evitar que vários CEs estejam diretamente ligados à ANV, centros intermediários de apuração, os CCs, coletam os resultados parciais dos CEs; de forma rústica, podem ser comparados aos Tribunais Regionais Eleitorais (Fig. A.1).

O estabelecimento de uma árvore de votação implica um protocolo para distribuição das chaves e coordenação das diversas autoridades de votação. Uma discussão de tal protocolo pode ser encontrada em [RBR97].

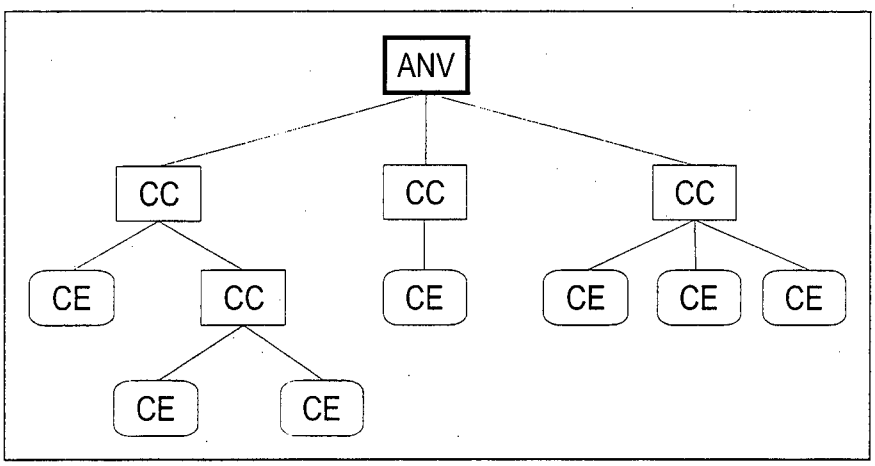

Figura A.1: Organização hierárquica de autoridades de votação

A.7 Autenticação de código

Um dos problemas mencionados em [FIL99] é o da garantia de que o programa que está sendo executado na urna é realmente equivalente ao código fonte auditado por terceiros. Uma forma de resolver parcialmente este problema é por meio da autenticação do código da urna. Neste caso, após a auditoria dos fontes, proceder-se-ia (ainda com o acompanhamento dos auditores) a assinatura digital do código fonte, a geração do código executável e a posterior assinatura digital deste código. A assinatura digital garante a integridade do programa, isto é, quaisquer alterações posteriores à assinatura são

detectadas, além da autenticação perante os que usam o programa, estes podendo saber que o programa que estão instalando ou executando é realmente o programa oferecido.

Entretanto, a assinatura digital dos programas envolvidos não resolve completamente o problema. Um programa em execução depende de alguns fatores que não são diretamente dependentes do código do programa. Entre estes fatores, pode-se citar as bibliotecas específicas utilizadas pelo programa, as bibliotecas padrão do sistema operacional, o próprio sistema operacional e o *hardware* em que ele é executado. Garantir a integridade de todos estes componentes não é uma tarefa trivial.

O desenvolvimento de programas seguros baseia-se no claro estabelecimento de quais são os pressupostos de confiança envolvidos, ou seja, quais as relações entre os componentes do ambiente computacional que podem ser consideradas seguras e quais são inseguras [VKP01]. Considere-se os dois locais principais onde são executados programas referentes à votação: o computador do votante e o servidor ao qual ele deve conectar-se. No caso do servidor, uma possível solução para este problema é o acompanhamento de todas as fases de instalação deste computador por uma equipe de auditores. Isto significa a obtenção do *hardware* de uma fonte confiável, a instalação de um sistema operacional também de fonte confiável, a instalação do ambiente de desenvolvimento, a compilação do programa fonte e a geração do código executável. Após o acompanhamento destes passos, pode-se homologar aquele computador em específico como confiável para executar o sistema de votação. Como garantia maior, pode-se também assinar os arquivos envolvidos, o que permite uma posterior detecção de alterações indevidas.

Por outro lado, é possível que um protocolo de votação digital impeça que, mesmo havendo problemas nos diversos programas que compõem o sistema de votação digital, nunca sejam violados os requisitos de segurança expostos em 5.2. Por conseguinte, o que pode ocorrer é uma votação anulada de forma parcial ou total, mas nunca a violação da privacidade do votante, por exemplo.

A.8 Gerenciamento de certificados e chaves privadas

Outra questão que deve ser explorada é a forma como certificados e chaves privadas são gerenciados nos vários locais onde são necessários.

No caso dos computadores dos votantes, podem ocorrer as seguintes situações:

- Se o sistema operacional instalado é o Windows, o próprio sistema operacional possui mecanismos para guardar e proteger chaves privadas e certificados digitais. Neste caso o componente do sistema de votação digital que será executado no computador do votante utiliza o conjunto de funções disponível na biblioteca CryptoAPI para ter acesso às chaves e certificados;
- No caso de outros sistemas operacionais, é necessário verificar e avaliar se existe algum mecanismo implícito para o gerenciamento de chaves e certificados, e possivelmente utilizar este mecanismo;
- Pode-se utilizar programas específicos para o gerenciamento de chaves e certificados. Por exemplo, o produto KeyMan desenvolvido pelo grupo alphaWorks da IBM [IBM01];
- Desenvolver programas que façam parte do sistema de votação digital e sejam responsáveis por este gerenciamento.

É importante lembrar que, além dos mecanismos técnicos para o gerenciamento de chaves privadas e certificados, é necessária a conscientização dos votantes com relação à importância da segurança destas informações. A segurança do sistema de votação digital também depende de as chaves privadas e certificados estarem seguros.

A.9 Não-disponibilidade de computador e Internet para os votantes

Para o caso de votantes que não possuam computador ou acesso à Internet, deverão ser disponibilizados computadores em locais públicos (tais como as seções eleitorais)

que possam ser usados como pontos de recepção de votos. Nestes computadores o gerenciamento de chaves é mais complexo, pois há vários votantes utilizando o mesmo computador. Uma possível solução é a utilização de *smartcards* pessoais.

A.10 Outros fatores

Há ainda outros fatores que não fazem parte do escopo deste projeto de pesquisa. Entre eles pode-se citar a disponibilidade dos computadores envolvidos, que depende diretamente da disponibilidade da Internet, assim como os ataques aos computadores, para os quais pode-se tomar medidas preventivas e corretivas.

Glossário

KR_A: chave privada de A

KU_A: chave pública de A

$E_K(M)$: informação M criptografada com a chave K

$H(M)$: resumo (*hash*) da mensagem M

$B_k(M)$: mensagem M ocultada pelo fator k

$S_A(M)$: mensagem M assinada com a chave privada de A; contém a mensagem (M) e a assinatura em si ($s_A(M)$)

$BS_A(M_k)$: mensagem M, ocultada pelo fator k, assinada cegamente com a chave privada de A; contém a mensagem (M_k) e a assinatura em si ($bs_A(M_k)$)

$MS_{\mathcal{X}}(M)$: mensagem M assinada com as chaves privadas de todos os elementos pertencentes a $\mathcal{X}$; contém a mensagem (M) e a assinatura em si ($ms_{\mathcal{X}}(M)$)

$MBS_{\mathcal{X}}(M_k)$: mensagem M, ocultada pelo fator k, assinada cegamente com as chaves privadas de todos os elementos de $\mathcal{X}$; contém a mensagem (M_k) e a assinatura em si ($mbs_{\mathcal{X}}(M_k)$)

AV: autoridade de votação; responsável por tarefas relacionadas à votação

AA: autoridade de alistamento, responsável por emitir os certificados de autorização para votar

AE: autoridade de escrutínio, responsável por garantir o trabalho honesto da autoridade de votação

$\mathcal{S}$: conjunto das autoridades de escrutínio

V: Victor, um votante

$voto$: seqüência de bytes representando um voto

$cedula$: seqüência de bytes representando uma cédula

$X \mid\mid Y$: seqüência de bytes X concatenada com a seqüência de bytes Y

LV: lista de votantes

$\#X$: número de elementos no arranjo X

RM: rede de mistura utilizada por V para enviar cédulas a AV de forma anônima

$\mathcal{A}$: arranjo de cédulas assinadas pelas autoridades de escrutínio

$\mathcal{A}_0$: arranjo inicial de cédulas contendo todas as possíveis combinações de votos, contendo k cópias de uma mesma cédula

$\mathcal{B}$: arranjo de cédulas assinadas pelos votantes

$RM_{\mathcal{A}}$: rede de mistura para o arranjo $\mathcal{A}$; eventualmente chamada de "urna"

$\mathcal{C}$: arranjo com todas as cédulas possíveis

$\mathcal{F}$: arranjo final de votos que devem ser apurados

`idvotacao`: número que identifica a votação

`id-idvotacao`: OID referente a `idvotacao`

DIR: diretório da votação; local onde estão armazenadas informações referentes a uma determinada votação

$A \rightarrow B : M$: A envia a mensagem M para B

Referências Bibliográficas

[AG97] ABADI, M.; GORDON, A. D. A calculus for cryptographic protocols: The spi calculus. In: *Fourth ACM Conference on Computer and Communications Security*. Proceedings. ACM Press, 1997, p.36–47.

[BEN87] BENALOH, J. D. C. *Verifiable Secret-Ballot Elections*. 1987. Tese (Doutorado) – Yale University.

[BRAa] BRASIL. Lei n. 4737, de 15 de Julho de 1965. *Institui o Código Eleitoral*. DOFC 19/07/1965 p.6746.

[BRAb] BRASIL. Lei n. 9504, de 30 de setembro de 1997. *Estabelece normas para as eleições*. DOFC 01/10/1997 p.21801.

[BRAc] BRASIL. Projeto de Lei n. 194/99, de 31 de março de 1999. *Altera a Lei 9504, de 30 de setembro de 1997, que "estabelece normas para as eleições" para ampliar a segurança e a fiscalização do voto eletrônico.*

[BY86] BENALOH, J. C.; YUNG, M. Distributing the power of a government to enhance the privacy of voters (extended abstract). In: *Proceedings of the 5th Symposium on Principles of Distributed Computing, Calgary, AB, Agosto de 1986*. Proceedings. New York: ACM, 1986, p.52–62.

[CAM97] CAMARÃO, P. C. B. *O Voto Informatizado: Legitimidade Democrática*. São Paulo: Empresa das Artes, 1997.

[CC96] CRANOR, L. F.; CYTRON, R. K. Design and implementation of a practical security-conscious electronic polling system. Washington University, Janeiro de 1996. Relatório Técnico WUCS-96-02.

[CER01] CERT. *CERT/CC Statistics 1988–2000.* Disponível em <http://www.cert.org/stats/cert_stats.html>, Março de 2001.

[CGJ+99] CANETTI, R.; GENNARO, R.; JARECKI, S.; KRAWCZYK, H.; RABIN, T. Adaptive security for threshold cryptosystems. In: Wiener, M., (Ed.), *Advances in Cryptology – Crypto '99: 19th Annual International Cryptology Conference*. New York: Springer-Verlag, v.403, 1999.

[CHA81] CHAUM, D. Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of the ACM*, 1981, v.24(2), p.84–88.

[DIF88] DIFFIE, W. The first ten years of public-key cryptography. In: *Proceedings of the IEEE*, v.76, Maio de 1988.

[ELEa] TRIBUNAL SUPERIOR ELEITORAL. *Regulamenta os atos preparatórios, a recepção de votos e as garantias eleitorais para as eleições de 2000.* Resolução n. 20563, de 27 de março de 2000.

[ELEb] TRIBUNAL SUPERIOR ELEITORAL. *Regulamenta a apuração e a totalização dos votos e a proclamação e a diplomação dos eleitos (eleições municipais de 2000).* Resolução n. 20565, de 27 de março de 2000.

[ELEc] TRIBUNAL SUPERIOR ELEITORAL. *Estabelece os modelos e uso dos lacres para urnas eletrônicas.* Resolução n. 20633, de 23 de maio de 2000.

[ELEd] TRIBUNAL SUPERIOR ELEITORAL. *Regulamenta a divulgação dos resultados das eleições de 2000.* Resolução n. 20676, de 11 de julho de 2000.

[FB97] FORD, W.; BAUM, M. S. *Secure Electronic Commerce.* Upper Saddle River: Prentice-Hall, 1. ed., 1997.

[FFW99] FEGHHI, J.; FEGHHI, J.; WILLIAMS, P. *Digital Certificates – Applied Internet Security*. [S.l.]: Addison Wesley Longman, 1999.

[FIL99] FILHO, A. B. A segurança do voto na urna eletrônica brasileira. In: *Simposio Sobre Seguranca Em Informatica'99*, 1999.

[FOO92] FUJIOKA, A.; OKAMOTO, T.; OHTA, K. In: Auscrypt '92, A practical secret voting scheme for large scale elections. In: *Lecture Notes in Computer Science*, p.244–251. New York: Springer-Verlag, 1992.

[GS93] GARLAN, D.; SHAW, M. An introduction to software architecture. In: Ambriola, V.; Tortora, G., (Eds.), *Advances in Software Engineering and Knowledge Engineering*, v.1, p.1–40. [S.l.]: World Scientific Publishing Company, 1993.

[HC01] HOFFMAN, L. J.; CRANOR, L. Internet voting for public officials: introduction. *Communications of the ACM*, v.44(1), p.69–71, Janeiro de 2001.

[HP00] HERNANDEZ, J.; PINTO, J. Especificación formal de protocolos criptográficos en cálculo de situaciones. *Novática*, v.143, p.57–63, Fevereiro de 2000.

[IBM01] IBM/alphaWorks. *KeyMan: another alphaWorks technology*. Disponível em <http://alphaworks.ibm.com/tech/keyman>, Janeiro de 2001.

[IETF01] Internet Engineering Task Force PKIX Working Group. *An Internet Attribute Certificate Profile for Authorization*. Disponível em <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ac509prof-06.txt>, Janeiro de 2001.

[ITU97a] ITU-T. *Recommendation X.509 (08/97) – Information Technology – Open Systems Interconnection – the Directory: Authentication Framework*, 1997.

[ITU97b] ITU-T. *Recommendation X.680 (12/97) – Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation*, 1997.

[JAK98] JAKOBSSON, M. A practical mix. In: *Theory and Application of Cryptographic Techniques*, p.448–461, 1998.

[KNU98] KNUDSEN, J. *Java Cryptography*. Cambridge: O'Reilly, 1998.

[LV00] LENSTRA, A. K.; VERHEUL, E. R. Selecting cryptographic key sizes. In: *Public Key Cryptography Conference*, 2000.

[MEA00] MEADOWS, C. Open issues in formal methods for cryptographic protocol analysis. In: *Proceedings of DISCEX 2000*, p.237–250. IEEE Comp. Society Press, 2000.

[MG01] MOHEN, J.; GLIDDEN, J. The case for internet voting. *Communications of the ACM*, v.44(1), p.72–85, Janeiro de 2001.

[MMS97] MITCHELL, J.; MITCHELL, M.; STERN, U. Automated analysis of cryptographic protocols using muroe. In: *1997 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, p.141–151., 1997.

[NSS91] NURMI, H.; SALOMAA, A.; SANTEAN, L. Secret ballot elections in computer networks. In: *Computers & Security*, v.10, p.553–560, 1991.

[RB99] RIERA, A.; BORRELL, J. Practical approach to anonymity in large scale electronic voting schemes. In: *Network and Distributed Systems Security, NDSS '99*, Internet Society, p.69–82, 1999.

[RBR97] RIERA, A.; BORRELL, J.; RIFÀ, J. A protocol for large scale elections by coordinating multiple electoral colleges. In: *Proceedings of the IFIP SEC '97 Conference*, Copenhagen, Maio de 1997.

[RBR98] RIERA, A.; BORRELL, J.; RIFÀ, J. An uncoercible verifiable electronic voting protocol. In: *Proceedings of the IFIP SEC '98 Conference*, Vienna-Budapest, Setembro de 1998.

[RIE99] RIERA, A. *Design of Implementable Solutions for Large Scale Electronic Voting Schemes*. Barcelona, 1999. Tese (Doutorado) – Autonomous University of Barcelona.

[SCH96] SCHNEIER, B. *Applied Cryptography*. New York: John Wiley & Sons, 2. ed., 1996.

[SK95] SAKO, K.; KILIAN, J. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth. In: *Eurocrypt '95, Lecture Notes in Computer Science*. New York: Springer-Verlag, p.393–403, 1995.

[SMI97] SMITH, R. E. *Internet Cryptography*. [S.l.]: Addison Wesley Longman, 1997.

[STA99] STALLINGS, W. *Cryptography and Network Security*. Upper Saddle River: Prentice-Hall, 2. ed., 1999.

[STI95] STINSON, D. R. *Cryptography – Theory and Practice*. Boca Raton: CRC Press, 1995.

[VKP01] VIEGA, J.; KOHNO, T.; POTTER, B. Trust (and mistrust) in secure applications. *Communications of the ACM*, v.44(2), p.31–36, Fevereiro de 2001.